AN INVESTIGATION INTO OPERATIONAL RISK MITIGATION IN THE UNITED ARAB EMIRATES COMMERCIAL BANKING INDUSTRY
CASE STUDY APPROACH

A Thesis Submitted in Fulfillment of the Requirement
for the Award of the Degree
Doctor of Philosophy

From

The University of Wales, Newport

By

Jamal Mousa Salim Shamieh

Newport Business School

United Kingdom

June 2011

DECLARATION

This work has not previously been accepted in substance for any degree and is not being concurrently submitted to candidature for any degree.

Signed.....(Candidate)

Date....24th June 2011.....

STATEMENT 1

This thesis is the result of my own investigations, except where otherwise stated. Other sources are acknowledged by footnotes giving explicit references. A bibliography is appended.

Signed.....(Candidate)

Date....24th June 2011.....

STATEMENT 2

I hereby give consent for my thesis, if accepted, to be available for photocopying and for inter-library loan, and for the title and summary to be made available to outside organiations.

Signed.....(Candidate)

Date....24th June 2011.....

ABSTRACT

This study researches a rapidly growing area of interest in the financial services industry, that is, operational risk management, with special focus on the mitigation phase. Operational risk management has accelerated in importance in the financial services over the last two decades for many reasons, not least of which is the well-known catastrophic failure of large banks such as BCCI, Barings and Indymac, as well as the recent Global Financial Crisis. One of the main drivers behind such bank failures was the failure of the banks' managements to manage effectively and efficiently their operational risk exposure. The focus of this study is operational risk mitigation in the United Arab Emirates Commercial banking industry.

A controversial issue with operational risk was deciding on an agreed and accepted definition within the financial services industry. It has been defined by Basel Committee on Banking Supervision as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk." This definition captures a wide spectrum of risk categories such as fraud risks, people risks, legal risks and compliance risks, to name a few.

Basel Committee on Banking Supervision, a Committee of banking supervisory authorities established by the central bank Governors of the Group of ten countries in 1974, published in June 2006 a document called the "*International Convergence of Capital Measurement and Capital Standards - A Revised Framework Comprehensive Version*" known as Basel II Accord, which requires banks, among many other things, to sustain capital adequacy to cover their operational risk exposures. This Accord was the result of a number of consultative documents issued by the same Committee which focused increasing attention on the need for operational risk adequate and efficient management. Bank managements are facing increasing pressure to ensure that operational risk exposures are being managed effectively and efficiently. This extended the main momentum for the study, being the first independently sponsored study of how the UAE commercial banks have developed their operational risk management frameworks as a basis for mitigating the range of operational risk exposures they encounter. The operational risks that prompted the current Financial Crisis and how they were mitigated in the context of the UAE commercial banks gave further momentum to the research.

The study addresses the various key players in operational risk management and is, therefore, inter-disciplinary. The foundations from which the field work was undertaken were based on theoretical propositions in the area of decision making since the process of mitigating an operational risk is rooted in making a decision. Multiple case studies were used in the design for the research to answer the research question and establish the practices in operational risk mitigation in the UAE commercial banking industry. Leading UAE commercial banks were carefully chosen as representatives of this industry.

The findings of the research are in line with the conclusions of Basel Committee on Banking Supervision that the main responsibility for operational risk management, and therefore mitigation, is vested in operational managers. The analysis demonstrates that they do not do this independently, but are supported by other experienced people in this field. A model and check-lists of operational risk management, and therefore mitigation, is proposed demonstrating the complexity of the whole process due to the nature and the scale of operational risks. The thesis concludes by discussing some further potential research suggestions in this ever-growing area of interest.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ACM	Association for Computing Machinery
AED	Arab Emirates Dirham
AMA	Advanced Measurement Approach
ATM	Automatic Transaction Machine
B2B	Business to Business
B2C	Business to Consumer
BBA	British Banking Association
Basel I	First Basel Accords
Basel II	Second of Basel Accords
Basel III	Third Basel Accord
BCBS	Basel Committee on Banking Supervision
BIS	Basic Indicator Approach
BOE	bank of England
BU	Business Unit
CA	Content Analysis
CBUAE	Central Bank of the United Arab Emirates
CCRC	Computer Crime Research Centre
CEBS	Committee of European Banking Supervisors
CEO	Chief Executive Officer
CIT	Critical Incident Technique
COSO	Committee of Sponsoring Organisations of the Treadway Commission
CRO	Chief Risk Officer
DA	Discourse Analysis
DSS	Decision support system
eCommerce	Electronic Commerce
FDIC	Federal Deposit Insurance Corporation
FSF	Financial Stability Forum
G10	Group of Ten
GCC	Gulf Cooperation Council
GDP	Gross Domestic Product
GT	Grounded Theory
IA	Internal Audit
IIA	Institute of Internal Auditors
IMF	International Monitory Fund
IT	Information Technology
KRI	Key Risk Indicator
mBanking	Mobile Banking
mBill Payment	Mobile Bill Payment
mWallet	Mobile Wallet
OCC	Office of the Comptroller of the Currency
OECD	Organisation for Economic Cooperation and Development
OpVaR	Operational Risk Value at Risk
OR	Operational Risk
ORF	Operational Risk Function
ORM	Operational Risk Management
P2P	Peer to Peer Transfer
PIN	Personal Identification Number
POS	Point of Sale
PEST	Political, Economic, Social and Technological
RA	Recursive Abstraction
SCAP	The Supervisory Capital Assessment Programme
TSA	The Standardised Approach
UAE	United Arab Emirates
US$	United States Dollar
USA	United States of America
VaR	Value at Risk
WSJ	Wall Street Journal

DEDICATION

To

Naila, Ilein and Fuad

You are my Success

Love to All

ACKNOWLEDGEMENTS

Many people have helped me during the last three years of researching operational Risk. For some, it may just have been a five-minute conversation about a particular point of concern, whilst others have been providing advice and encouragement throughout. I am grateful to them all.

I have been especially fortunate with my supervisors who have provided me with constant support throughout. Acting out the roles of friend, critic, mentor or coach (to name but a few) is no easy task when one is busy with a multitude of other work pressure. Dr. Jonathan Deacon, Dr. Stuart Metcalf and Dr. Andrew Thomas have been a constant source of inspiration with their help, encouragement and attention to the detail...Dr. Munir Lutfi, has guided me throughout the process, kept me focused in the right areas and offered support whenever I have asked for it. I am grateful to you all.

Having been in management myself, I know first-hand how busy and demanding the job can be. Managers are busy people. I am grateful to all those in the banks I have worked with who found the time to meet with me. An extra word of thanks goes to those who acted as the main contact and organised all the diary arrangements. Without your help this study would never have been completed

Finally, I would like to thank my wife, Naila, for the unequivocal support she has shown whilst I have been undertaking this research. I could never have gone through this process without your love, patience and understanding.

1. INTRODUCTION

This Chapter provides background to the research and introduces the research main and secondary questions as well as the researcher's objectives. The methodological framework for this study, the case study approach, along with an overview of the research design are outlined. The Chapter concludes with an important part, that is, a discussion of the 'Contribution to Knowledge' followed by the structure of the thesis.

1.1 Background to the Research

1.1.1 Basel Committee on Banking Supervision (BCBS)

> "In order to encourage better risk management practices, the Committee is keenly interested in efforts by financial institutions to effectively manage and mitigate operational risks."

This quote from the operational risk Consultative Document (BCBS[1] 2001, p. 12) to BCBS (2004) Capital Accord captures both the aim (encourage better risk management practices) and focus (operational risk mitigation) of this study.

Basel Committee on Banking Supervision (BCBS) published its first Capital Accord: "*International Convergence of Capital Measurement and Capital Standards*" in 1988

[1]BCBS is a committee created in 1974 by the Central Bank Governors of the Group of Ten nations. The purpose of BCBS is to encourage convergence toward common banking approaches and standards. It formulates broad supervisory standards and guidelines and recommends statements of best practice in banking supervision in the expectation that members' authorities and other nations' authorities will take steps to implement them through their own national systems (Marrison 2002).

(BCBS 1988). This Accord addressed credit risk[2]. A revised edition that addressed market risk[3] was published in 1996 (BCBS 1996), hereafter; referred to as Basel I[4].

BCBS published its second Capital Accord to address operational risk (OR): *"International Convergence of Capital Measurement and Capital Standards"* in 2004 (BCBS 2004), and revised editions in 2005 (BCBS 2005a) and 2006 (BCBS 2006) hereafter; referred to as Basel II[5]. Basel II is now enforced in most countries in the world (Moosa 2007).

Recently, BCBS published its third Capital Accord in December 2010: *"International Framework for Liquidity Risk Measurement, Standards and Monitoring"* in response to the deficiencies in the financial regulation revealed by the Global Financial Crisis from liquidity risk[6] perspective, hereafter; referred to as Basel III[7]. Nevertheless, in this study, there will be more focus on Basel II for two reasons:

---

[2] The Business Dictionary defines credit risk as an investor's risk of loss arising from a borrower who defaults payment.

[3] The Business Dictionary defines market risk as the risk that the value of a portfolio, either an investment portfolio or a trading portfolio, will decrease due to the change in the value of the market risk factors. The four standard market risk factors are stock prices, interest rates, foreign exchange rates, and commodity prices.

[4] Basel I is the first of the BCBS Accords, primarily focused on credit risk and later was revised to include market risk. Assets of banks were classified and grouped in categories according to the credit risk they carry (Marrison 2002).

[5] Basel II is the second of the BCBS Accords, addressed credit risk, market risk and OR, and primarily focused on recommendations on banking regulations. The purpose of Basel II is to create an international standard that banking regulators can use when creating regulations about how much capital banks need to allocate to guard against the types of risk banks face (Basel II).

[6] The Business Dictionary defines liquidity as the risk that a given security or asset cannot be traded quickly enough in the market to prevent a loss or make the required profit.

[7] Basel III is the third of the BCBS Accords focused on strengthening bank capital requirements and introduces new regulatory requirements on bank liquidity risk (Basel III).

1. Basel II is more concerned with operational risk management, measurement, sources and other operational risk areas (Basel II, p. 140 - 152); whereas, Basel III is concerned mainly with liquidity risk management (Basel III, p. 1).
2. Basel III is not due for final implementation, yet. It will officially be introduced in two stages: January 2015 and January 2018. Until then, Basel III will undergo analysis of financial institution feedback, monitoring and updating (Basel III, p. 41).

During the last twenty, years many changes and developments have taken place in the banking industry. The failure of major banks such as BCCI, Barings and Société Générale [8] as well as many other major bank failures (See Robertson and Austin 2008 for a comprehensive list of bank failures during the last twenty years[9]) demonstrate the consequences and dangers of not managing Operational Risk efficiently and effectively. Since the beginning of the recent financial crisis that started in the year 2007, (hereafter referred to as the Financial Crisis) and up to 31st Dec. 2010, the updated 'failed bank list' of FDIC (2010) contains 155 failed banks in the Unites States of America (USA) alone.

Recently, a paper published by the Bank of England (BOE) indicates that as a result of the Financial Crisis the global banking system has arguably undergone its biggest episode of instability since the start of World War I (BOE 2008).

---

[8] For a detailed analysis of BCCI case see Kerry and Brown (1992) and Angelos (2005), Barings case see McConnell (1998), for a perpetrator's view of the Barings case see Leeson (1996) and Société General see Rayner and Allen (2008).

[9] In the history of United Arab Emirates banking industry, there has been no records of bank failures except for the non-UAE bank known as Bank of Credit and Commerce International (BCCI) which merely had a branch in UAE (see Kerry and Brown (1992) and Angelos (2005) for a good illustration of the BCCI case).

Preparations for this research project commenced prior to the beginning of the Financial Crisis, which prompted the Dubai debt crisis[10] (hereafter referred to as the Dubai Crisis, and both the Financial Crisis and Dubai Crisis will together be referred to as the Financial Crises) in the United Arab Emirates (UAE). Nevertheless, the Financial Crisis could be predicted (Patrick 2010). The author of this thesis argues that since the Financial Crisis severely impacted developed countries with the most sophisticated financial systems, it could also impact developing countries, such as the UAE, due to less mature financial systems. The implication is that there is a greater need to understand the operational risks that have contributed to the Financial Crisis, which seem to have been under estimated, and how they were mitigated, and keep an 'open eye' to examine the operational risk mitigation processes in order to predict and prevent recurrence of similar crises (Lilico 2008).

Diversification in the UAE commercial banking illustrates the extent to which banks are moving into new business areas, such as stock wallets, insurance and real estate financing. A drawback is that new business areas come with risk imbedded in them, for various reasons (such as using new information technology (IT) applications) hence, instigating additional risks (As-Sardi 2009).

[10] With the onset of the Financial Crisis, Dubai's real estate market declined after a six-year boom while the UAE commercial banks were extending loans at bubble pricing. Dubai government asked all providers of financing to major real estate firms to extend the debt maturities, which exceeded U.S.$59 billion. As a result, thousands of employees were laid off and banks lost liquidity; resulting in a stalled economy in Dubai (Smith and Kiwan 2009).

Basel Accords recognise the changing banking environment, and are focused at ensuring that all banks sustain regulatory capital adequacy sufficient to counteract the underlying risks they face, irrespective of the source (Moosa 2007a).

1.1.2 Framework for Risk Management

A survey conducted by the author revealed that Basel II incorporates the phrase 'risk management framework' on ninety eight occasions. The author would contend that such emphasis highlights the importance of the risk management framework in the banking industry. The undertaken literature review supports this view.

As early as the year 1919, in his 'Administration industrielle et générale'[11], Fayol (1919, p. 3) classified the various activities of a company in six groups:

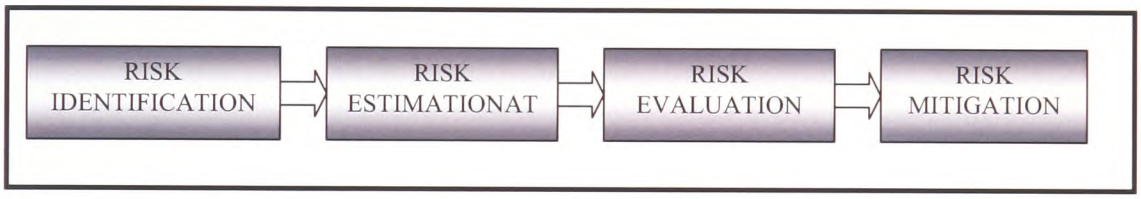
1. Engineering, production, manufacturing and adaptation: Technical Group.
2. Buying, selling and exchanging: Commercial Group.
3. Searching for and optimising use of capital: Financial Group.
4. Protection of assets and personnel: Security Group.
5. Stocktaking, balance sheets, costing and statistics: Accounting Group.
6. Planning, organising, commanding, coordinating and controlling: Managerial Group.

The objective of the Security Group as he discussed it was to safeguard property and persons against theft, fire and flood, to ward off strikes and felonies and broadly all social

[11] An English translation appeared in 1929 with a revised edition some twenty years later (Fayol 1949).

disturbances liable to endanger the progress and even the life of the business (Fayol 1949, p. 4). Subsequent researches that placed Fayol's work within today's standards of management theory identified a component of security as being risk management, involving: risk exposure identification, risk estimation, risk evaluation and risk control and financing (Rodrigues 2001), summarising a framework for the management of risk within an organisation. Other authors[12] (White 1995, Parker 2005, Millo and MacKenzie 2007 and Jason 2009) identified a similar concept, which may be summarised in Figure 1.

Figure 1: Simple Risk Management Model



Source: Parker (2005)

Parker (2005, p.61) explains these terms as:

Risk Identification: Perceiving hazards, identifying failures, recognising adverse consequences;

Risk Estimation: Estimating risk probabilities, describing the risk, quantifying the risk;

Risk Evaluation: Estimating the impact of the risk, judging acceptability of the risk, comparing the risk against benefits;

[12] The terminology may differ between the authors but as Millo and MacKenzie (2007) note, there is considerable agreement about the components of the model even if the labels are different.

Risk mitigation: The action taken once the identification, estimation and evaluation processes have taken place.

Andreas (2007) maintains that the principal objective of the risk management framework is to adjust the level of risk faced by a business until it is acceptable in terms of the risk reward criteria adopted by the organisation's Board[13]; with the intention of maximising the positive impact and minimising the negative impact.

It can be argued that all aspects of risk within an organisation need to be encompassed by risk management. A review of the literature identifies a range of business risks[14], and a growing interest is being demonstrated by the established consultancy firms[15] in the generic area of risk management framework. The first issue faced by an organisation that wishes to manage its total business risk exposure is to decide what types of risks are included in its own business environment (Alexander 2005). A recent survey report indicates that firms are yearly losing considerable amounts of money due to risk management failures (Robertson and Austin 2008).

[13] The Business Dictionary defines the Board of an organisation as a body of elected or appointed members who jointly oversee the activities of an organisation. Sometimes, it has different names, such as Board of Trustees, Board of Governors, Board of Managers, or Executive Board. It is often referred to as the 'Board.'

[14] The term business risk includes all risks faced by an organisation such as market risk, credit risk, operational risk, strategic risk and reputational risk (Alexander 2005).

[15] An example is the risk model produced by The Public Risk Management Association (2010).

1.1.3 What is Operational Risk?

Basel II produced a revised definition for operational risk which has found reasonable acceptance in financial institutes. A 'recent' definition seems to be somewhat inconsistent given that operational risks have existed in organisations for many years (Moosa 2007). Banks were in the practice of producing their own operational risk definitions. However, the majority of banks have recently adopted the Basel II definition as a workable definition (Moosa 2007, Dorfman et al. 2008, Hubbard and Douglas 2009). Basel II adapted the definition produced by the British Banking Association and Price Waterhouse Coopers (BBA 1999a), thus:

> "Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk" (Basel II, p. 140).

The author would contend that the use of the word risk in the Basel II definition of operational risk implies that the reader is supposed to have an understanding of the concept of risk in the first place, which is unhelpful when defining a term.

The definition of operational risk illustrates that it has a three dimensional focus, thus; a loss resulting from a breakdown (failure) in the internal controls (systems/processes) that should be designed to mitigate the risk in the first place. The breakdown may occur for different reasons, including, as quoted, processes, people and system failure. Equally, a breakdown can occur due to lack of controls in place to reduce the possibility of the risk occurrence. The definition also recognises the effect that external events can have in giving

rise to operational risk. External events might include systemic risk[16] affecting multiple institutions simultaneously with broad consequences (BBA 1999a).

This definition also focuses exclusively on the negative aspects of risk. 'Positive' risk, whilst probably self-contradictory from a linguistic point of view, may not be considered an appropriate concept in the context of operational risk; although under certain circumstances the operational risk mitigation decision may be beneficial (positive risk-taking), for example, outsourcing and legal risks. This is a view shared by Holtgrave and Weber (2009).

1.1.4 Bank Selection Criteria

> "Operational risk exposure is inevitable and can be acceptable as long as we understand the concepts behind it and we are confident that it's not always cost effective to the business to introduce additional controls."

The above quote by one of the Risk Managers interviewed in this research captures the essence of operational risk management (ORM). This study focuses on ORM in the UAE commercial banks, with particular emphasis on the mitigation phase. The UAE commercial banking industry has been chosen for the following reasons:

[16] The Business Dictionary defines systemic risk as the risk of a potentially catastrophic financial system instability, caused by certain events or conditions in financial intermediaries (such as exposure to other industry participants, physical or natural disasters, or a change in regulations, laws, accounting or taxation beyond the organisation's control). It refers to the risks imposed by inter-linkages and interdependencies in a system or market, where the failure of a single entity or cluster of entities can cause a cascading failure, which could potentially bankrupt or bring down the entire system or market.

1. The Global Financial Crises emphasised the need to understand the operational risks that the UAE commercial banks are facing and how the recurrence of such crises can be predicted and mitigated in a timely manner;
2. There is growing pressure on the Regulators of the UAE banks, the Central Bank of the United Arab Emirates (CBUAE), to ensure that they inspect the adequacy of Banks' risk management frameworks and internal control mechanisms (Basel II) to counteract operational risk exposures;
3. The corollary of the latter point is the growing pressure on the Senior Management[17] of the UAE commercial banks to ensure that it establishes adequate risk management frameworks and internal control mechanisms to counteract operational risk exposures;
4. The UAE commercial banks are likely to have a wide range of operational risks since they have a wide range of products and systems within which operational risks may reside;
5. The multi-cultural population of the UAE is unique in its extremely diverse origins. According to the World Fact Book (2009), the demographic structure of the UAE population is extremely diverse, consisting of: Emirati 19%, other Arab, Iranian, South Asian (Indian, Pakistani, Bangladeshi, Sri Lankan) 50%, and other expatriates (including Westerners and East Asians) 31%. Hence, due to the large number of people and systems involved in the UAE commercial banking sector, the opportunity of operational risk occurrence is high. Nevertheless, the author

[17] The Business Dictionary defines Senior Management as individuals at the highest level of the organisational management who have the day-to-day responsibilities of managing an organisation and hold specific executive powers conferred onto them by the authority of the Board.

would contend that this multi-cultural diversity may instigate a wide spectrum of ORM skills.

6. The author's knowledge of the dynamics of the UAE commercial banking industry.

Despite the fact that the literature review did not identify any prior work on operational risk mitigation in the UAE commercial banks, operational risk was chosen since a number of authors have confirmed the view of Tschoegl (2005) that ORM is still in its infancy (Dorfman et al. 2008). Much of the academic literature concerning the management of banking risks has focused mainly on market risk and credit risk as main concerns with recent increasing attention to operational risk (Hubbard and Douglas 2009). Such increasing attention makes operational risk an interesting and fruitful area for research since it relates to practical and current problems facing the management of the commercial banking industry.

Risk mitigation in the UAE commercial banks was selected in order to focus the research into one area which could be seen as one of the most important daily challenges facing management, that is to say, how best to manage the operational risk exposures identified through the risk management processes. Risk identification, estimation and evaluation are all important phases of risk management, but unless conscious risk mitigation strategies are deployed, it may all be in vein. The fact of not having effective risk mitigation strategies can be catastrophic as was highlighted by the cases of BCCI, Barings and Société General, to name a few. As pointed out by Agence France-Presse (2008), in financial terms, the Société General case was the result of the ultimate but ill-developed management

processes, coupled to an IT genius, at the expense of ORM. *Appendix A* provides an example of a brief case study on a well publicised operational risk incident which affected the UAE commercial banks (The credit card fraud case). The incident is useful to examine because it is in the public domain, has a significant impact and provides a good opportunity to examine the mitigating tactics used.

1.2 Research Framework

1.2.1 Lack of Prior Research

According to Blommestein and Peters (2009), ORM of financial institutions is a topical subject from the perspectives of both academics and practitioners. Grody and Toms (2009) argue that academics encounter sever difficulties in ORM research due to the limitations of obtaining hard empirical data.

Operational risk can be viewed as the unwanted future event which, on small scale, can happen on a daily basis but which, when it hits the headlines, can lead to firms losing significant sums of money (Angelos 2005). As was witnessed by the events of BCCI and Barings, the consequences of inadequate ORM can even lead to the collapse of the whole bank. The fact that inadequate ORM, and in particular; inadequate operational risk mitigation can lead to an impact on the bottom-line further highlights the importance of research into the area of operational risk.

A review of the literature did not find any work dealing with operational risk mitigation in the UAE commercial banks. However, notable work was found that deals with risk

mitigation strategies in the banking industry in general, including work related to operational risk mitigation (Kaple and Gregory 2006, Moosa 2007)). In a paper by Currie (2004, p.14), operational risk is defined as "the problems associated with accurately processing, settling, and taking or making delivery on trades in exchange for cash. It also arises in record keeping, computing correct payment amounts, processing system failures, and complying with various regulations." This bouquet of activities suggests that there is no one best way to mitigate operational risk and there is unlikely to be any consensus about the most appropriate way forward.

1.2.2 Focus of the Research

The origins of the term 'commercial bank' in the UAE can be traced back to 1980 when the Central Bank of the United Arab Emirates created a new commercial bank group in accordance with the UAE Federal Low (10). The requirement to being in this group was the provisioning of commercial banking services. Further insight was given by the CBUAE when 'commercial banks' was a group which broadly comprised banks having extensive branch networks in the UAE and offering commercial services (CBUAE 1990). All such banks are supervised by the CBUAE, and any new comer entering into this category would have to be authorised by the CBUAE to conduct such business[18].

Islamic banks have been excluded due to the special nature of their operation. This does not, of course, preclude expanding the research into such banks at a later stage.

[18] This is a requirement of the UAE Federal Law No. (10) of 1980.

The research examined four UAE commercial banks, and using well-established case study methodology, explored the operational risk mitigation processes employed. The research was concerned with how the UAE commercial banks mitigated their operational risk exposures and focused on modelling the processes involved.

1.2.3 The Research Questions

Finken and Silke (2004) note that once operational risks have been identified and assessed, all techniques to mitigate the risk fall into certain categories, and when managers have to decide on how best to mitigate risks, they will normally have multiple risk mitigation strategies available to them. (Kaple and Gregory 2006, p. 38), for example, identified five ways of controlling (mitigating) risk situations:

1. Risk avoidance;
2. Risk assumption (by virtue of the nature of the activity);
3. Risk reduction;
4. Risk transfer;
5. Combination of the above.

On the other hand, Dorfman and Marks (2007, p.9) argue that once risks have been identified and assessed, all techniques to mitigate the risk fall into one or more of the following categories:

1. Risk avoidance (eliminate, withdraw from or not become involved);
2. Risk reduction (optimise and mitigate);
3. Risk sharing (transfer, outsource or insure);

4. Risk retention (accept and budget).

In essence, these risk mitigation strategies are almost identical in purpose, and managers themselves, also have their own risk-taking behaviour patterns (Mok and Hagel 2004). Further, managers must also take due consideration of the nature of the risk being mitigated, the risk aptitude of the business in which they work, the time available to effect the mitigation action and the cost of the potential risk mitigation solution (Mok and Hagel 2004). This provides an interesting bouquet of ingredients from which a risk mitigation decision must be taken, even if the decision is 'to do nothing' and thus accept the risk.

In an attempt to investigate and understand better the processes used, the main research question is:

How do the UAE commercial banks mitigate their operational risk exposures?

A number of secondary questions evolve from this main question. These questions involve:

- Areas of mitigation responsibility;
- Establishment of mitigation tactics;
- Communication of risk management decisions;
- Barriers to mitigating operational risk.

It was hoped that answers to these questions would shed light on how seriously the UAE commercial banks are taking the proposals on operational risk emanating from the leading

world banking supervisory body, the BCBS. It would also establish whether operational risk mitigation can be modelled as a basis for extending the risk management model to include the other risks faced by the commercial banking industry.

1.3 Research Design

1.3.1 Case Study Methodology

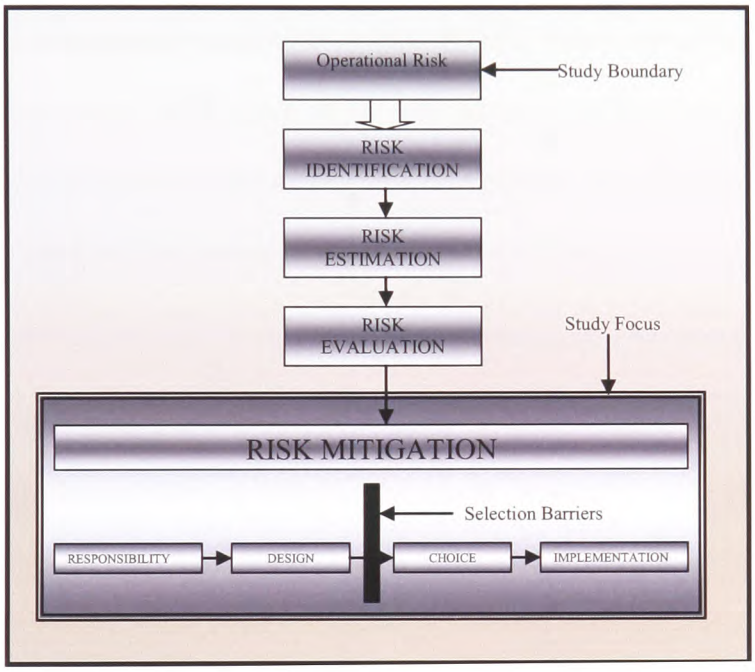
The use of qualitative research methods and the inherent strengths that they bring are becoming more widely accepted (Thomas 2004), and the metaphysical polemics (principles of reality arguments) concerning epistemological (that of theory of knowledge/philosophy) techniques are growing in their intensity (Hunter and Erin 2008). Dul and Hak (2008) argue that case study methodologies are now well-developed, articulated in the literature and are highly appreciated when the research questions are 'how' and 'why'; where the focus is on contemporary events; the research is exploratory or descriptive. The data was collected using multiple exploratory case studies, which are favoured for answering such research questions (Baxter and Jack 2008, Dul and Hak 2008). Multiple case studies also enabled the author to compare management practices in the area of operational risk mitigation.

1.3.2 An Overview of the Research Design

The research methodology used in this study involved developing a preliminary model of the risk mitigation process based on the literature review, and exploring adherence to the model. The preliminary model is an extension of the risk management model in the risk mitigation phase. The extension is based on an appropriate decision making model, driven

from the literature (Simon 1997 and Lurie 2004), since the act of mitigation involves making a decision about how to reduce the probability or lessen the impact of the risk. The model is shown in Figure 2.

Figure 2: Preliminary Operational Risk Mitigation Model



Source: Developed by the author

Data was collected using primarily semi-structured interviews, together with papers and documents concerning the bank and its approach to ORM. Data triangulation was employed, using *Critical Incident Techniques* (CIT's) to validate the results since CIT's provide data that can be used to either substantiate or reject the propositions concerning operational risk mitigation (Serenko 2006).

The section dedicated to the research methodology examines in detail the qualitative analysis employed, justification for choosing particular techniques; as well as the research design.

The literature review carried out prior to the field work identified the main players who assist operational management to mitigate operational risk, hence; Risk Managers. Also, it identified a role for Internal Auditors in this regard. These two groups together with the Operational Managers were the units of analysis for the study. The research was carried out between January 2008 and December 2010.

1.4 Scope of the Research

The 'boundary' (Cash and William 2002) for this study was ORM, whilst the 'focus' (Cash and William 2002) was one phase of ORM, namely operational risk mitigation.

The author recognises that there are other risks within banks, for example market risk and credit risk, but they have not been the centre of attention in this study; although the critical reader may note that there are occasions when the boundaries between these risks are not a clear cut (Alexander 2005). The fact that the research questions are aimed at exploring the operational risk mitigation phase did not preclude the examination of other phases of ORM. They were included in the study but were not discussed in any greater detail, except for where there was some linkage to operational risk mitigation.

An area of operational risk that has attracted a significant amount of attention over the last few years is ORM (Moosa 2007). This is concerned with the identification, estimation evaluation and mitigation phases, including the measurement and quantification of operational risk exposures. The author discussed ORM in very broad terms at the interviews to substantiate the link between quantification and mitigation. The generic area of operational risk quantification is, however; outside the scope of this study. The emphasis on the UAE commercial banks did not preclude the author from examining ORM in other operations, such as enterprise risk management. This was done to broaden the author's knowledge base and literature review as there is very little to be found in the current literature about ORM in the context of the UAE commercial banks.

1.5 Positioning of the Researcher: the Researcher's Objectives

From the outset, the researcher aimed at building a model for operational risk mitigation actions that would be of interest and use to policymakers, regulators and those in charge of the banking corporate governance, as discussed in the section 1.6 dedicated to the 'Contribution to Knowledge.'

Models that are generated from academic research should have pragmatic validity, according to Collins and Joseph (2004). By this they mean they should be useful and user friendly. Thus, building a model of the risk mitigation process to encourage better ORM practices is considered an important output.

Weik (1995) describes the process of model building as being iterative where one is continually speculating and abstracting using the data that has been collected. The model development will be discussed in more detail in section 2.1.4.

The researcher aimed to achieve other secondary objectives, thus; a high level review document for auditing the emerging Operational Risk Functions, a practical 'road map' of how to approach operational risk mitigation, and better understanding of management in major financial institutions. The objectives of the research will be discussed in more detail in the section dedicated to 'Contribution to Knowledge' (section 1.6)

ORM is, or at least should be, of interest to every manager, whether they work in the financial services or otherwise. The cost of ORM failures in all industry sectors can be measured not only in monetary terms, but also sadly in terms of people's lives (Gustafsson 2007). As a result of this research project, the profile of ORM and therefore operational risk mitigation will be raised.

1.6 Contribution to Knowledge

Operational risk is an area that is not researched in the UAE, and is of growing importance to financial institutions because of regulatory requirements. The study examines an uncharted area in the UAE with a practical orientation towards managing operational risk on a day-to-day basis. Whilst the focus of the study has been in the UAE, it has international implications because BCBS is an international organisation responsible for bank regulation. The researcher aimed at building a research model that would be of

interest and use to policymakers, regulators and those in charge of the banking corporate governance. In particular, this model is expected to contribute to the area of operational risk mitigation in the banking sector.

There is mounting pressure from BCBS, both on the regulators of the UAE banks and Senior Management within the banks, to mitigate operational risk exposures effectively (Saif and Choucair 2009). BCBS is also mandating banks to boost market discipline through enhanced disclosure (Basel II). This mandate requires disclosure of the bank's risk assessment methods, an area which the research has examined in relation to operational risk. The development of a model for operational risk mitigation actions will provide an important contribution to how the UAE commercial banks will tackle this problem and help to identify what shall be current practice. The development of a practical 'road map' of how to approach operational risk mitigation will provide an important contribution to those managers[19] who are seeking to improve their understanding of the process. Furthermore, the development of a high level review document for auditing the emerging Operational Risk Functions will help to provide comfort that such functions are doing their job effectively.

As recognised by Basel II, studying how banks mitigate operational risk will be an important contribution to helping banks reduce the exposure, frequency or severity of an operational risk incident. Reducing fraud, errors and inefficient operations through effective operational risk mitigation will have a positive effect on an organisation's cash

[19] Manager means principally operational management but equally well applies to risk managers.

flow and help to improve a risk awareness culture in the business, which should ultimately lead to an increase in shareholder value[20]. Additionally, this research will provide a contribution to the understanding of management in major financial institutions, particularly from a Board perspective, where the pressure to demonstrate effective corporate governance continues unabated. This is particularly so in the UAE environment with the recent emphasis being placed by the CBUAE mandate on ORM.

Given the lack of research in the area of operational risk in the UAE, it is hoped that the research will contribute to the construction of a cumulative knowledge vis-à-vis ORM, operational risk mitigation and the processes and tactics used to mitigate operational risk. The research is very much at the exploratory stage. No prior work was found to have been undertaken in this area in the UAE. Methodologically, the study contributes to the growing repository of case study research programmes in another area of business that is ORM, and may be viewed as a building block on integrated or comprehensive risk management.

1.7 Structure of the Thesis

The thesis has been structured in the following way:

- Chapter 2 provides a comprehensive review of the related literature and discusses why operational risk is important and why a 'preliminary model' of the risk mitigation process was chosen. Related theoretical propositions are summoned when necessary and as relevant, in this Chapter;

[20] Shareholder value is an analysis valuation approach which considers in broad terms that the value of a business to a shareholder can be determined by discounting its future cash flows using an appropriate cost of capital (Eldomiaty 2005).

- Chapter 3 argues for the methodological position adopted and provides the research design;
- Chapter 4 provides the study findings emerging from the detailed data analysis work and provides related explanations;
- Chapter 5 discusses the implications for management, focusing particularly on ORM;
- Chapter 6 summaries the research and identifies the limitations and suggested areas for further research.

2. LITERATURE REVIEW AND THEORETICAL PROPOSITIONS

This Chapter covers the literature review and aims to build a theoretical foundation upon which the research is based. Relevant literature is reviewed and issues related to the topic being studied are identified. It begins with introductory comments concerning the areas of knowledge being reviewed. Each area is then examined separately in more detail.

An extensive state of the art of literature review is discussed in chronological order from the earlier studies to the most recent literature on the subject; unless the context dictates otherwise.

2.1 Introduction

2.1.1 Disciplines Covered by the Literature Review

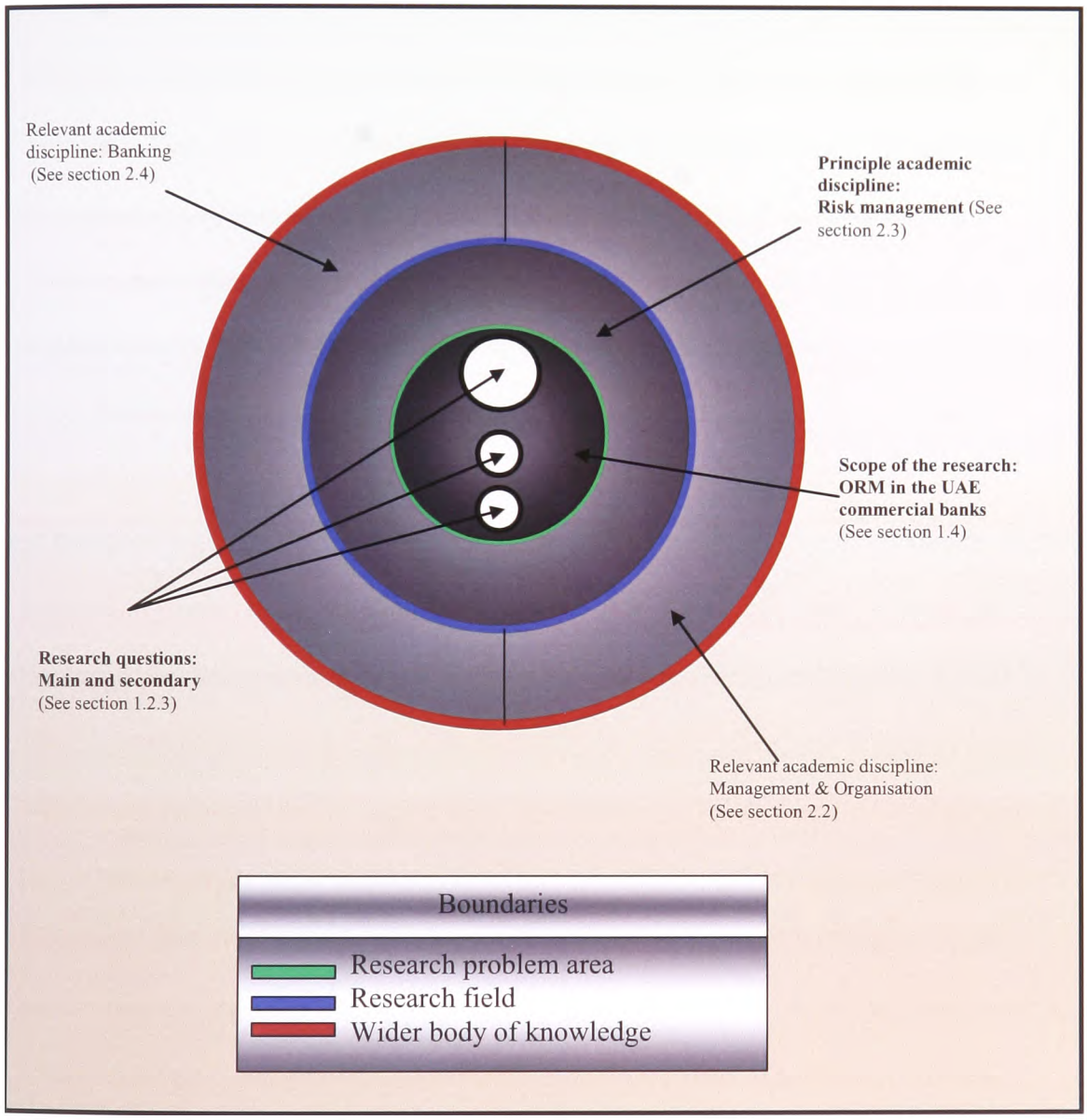
The research is based on the following academic disciplines:

1. Management and Organisations: The decision-making environment and the organisational arrangements for operational risk mitigation;
2. Risk Management: The discipline where the literature review has been focused and, in particular, the regulatory environment, the control framework and the role of Internal Audit in the internal control framework;
3. Banking: The current issues facing the UAE commercial banking sector and how they may impact upon ORM;

Figure 3 illustrates diagrammatically how the research questions link to the wider body of knowledge. The outer layer represents the wider body of knowledge, and this and the other

layers may be peeled back to arrive at the core of the research problem, i.e. the research questions.

Figure 3: The Boundaries and Academic Disciplines of the Study



Source: Developed by the author

2.1.2 Focus on Risk Management: Contingency Theory

Considering that the core discipline underpinning this research is risk management, a few introductory words that reflect on its history and identify its theoretical positioning, are considered appropriate to place the research into context.

Bernstein (1996) discusses how a mere 350 years separate today's risk management techniques from decisions guided by superstition, blind faith and instinct. The notion of risk management by instinct can be seen throughout the history of civilisation. For example, early man feared attack from animals so mitigated that risk by living in a cave, and the Romans feared insurgence so mitigated that risk by maintaining a big well-trained army. Risk management is, therefore, nothing new and more recent times have seen increasing sophistication in the development of risk management techniques.

Earlier, Lavington (1925) developed an approach to the theory of business risk based on the economic view point of satisfying material needs and the inherent problems, or business risks, in attempting to achieve these needs. His theory was built on two conditions which affected production within an organisation: the intractability (difficulty in manipulating) of the natural resources at the organisation's disposal, and the incalculability (difficulty in foreseeing) of the results of the operations by which these resources are adapted by the organisation to produce goods and services for the society. He concludes that business risks consist of the probability of occurrence of losses which arise from incalculability. He, therefore, places the emphasis of risk management within the operations of the organisation where the goods and services are produced.

More recently, McConnell (1996) in his review of major risks of international banking notes how the risk management function performs a similar role to the traditional control functions in the techno-structure[21] part of the organisation, and that one of their primary roles is that of problem identification and formulation.

Risk management is also concerned with influences outside the firm, in particular, the environmental conditions within which the firm must operate. Hatch (2002) notes how rapidly changing environments require organisational flexibility giving rise to organic organisations[22], because like other living things, they adapt flexibly to changing circumstances. At the opposite end of the spectrum are mechanistic organisations which Hatch (2002) points out existed in stable environment where the need is for specialisation of the tasks and jobs undertaken, thus creating a high-performance and disciplined or mechanistic system.

The decision as to when to use either the organic or mechanistic form of organisation is an example of contingency theory (Hatch 2002). Contingency Theory is a behavioural theory that claims that there is no ideal way to organise and lead a company, or to make decisions Instead, the optimal course of action is contingent (dependent) upon the internal and external business environments (William 2001). Cade (2002) argues that risk management and the framework within which risk management takes place are rooted in contingency

[21] The functions of the techno-structure operate at all levels of the organisation by analysing activities of the workers in the operational core, planning and carrying out studies of managerial tasks and planning and developing control systems for Senior Management (Mintzberg 1989).

[22] A term created by Burns and Stalker in the late 1950's. Organic organisations, unlike mechanistic organisations, are flexible and value external knowledge (Burns and Stalker 1961).

theory since the process of risk identification (the first phase in the risk management process) takes place within a two dimensional framework within the business environment in which the firm operates: the likelihood of the risk (risk estimation) against its possible impact (risk evaluation). Risk mitigation, the phase that follows, must take due consideration (is contingent upon) of the probability and impact as part of the information from which a risk mitigation decision will have to be made Cade (2002).

2.1.3 Sources of Literature

In order to provide a broad ranging view of the disciplines, the literature has been selected from both academic and practitioner sources. The emphasis has been on academic material, but the reader should note that there is also a reasonable number of relevant practitioners' references.

2.1.4 Model Building

Weik (1995) describes the process of model building or development as being iterative where one is continually speculating and abstracting through the process using the data that has been collected. The resulting model should be composed of assumptions, abstract reasoning, and speculation which describes or explains an observed or experienced phenomenon's constructs (terms which may be applied or even defined on the basis of the observables), their interrelationships, and their boundaries Weik (1995). An analogy was also cited by Baert and Carreira (2005). The operational risk mitigation model developed in this study is based on this process.

The building of a model is of extreme importance to researchers because it can serve as a basis for accumulating and refining knowledge in the domain of interest (Thomas and James 2006). Since one of the objectives of this research is to present a model of operational risk mitigation, a few words on what model building is, are presented in this section.

Bell (2008) describes the purpose of a building a model as to organise efficiently and to communicate clearly. Epistemologically (from knowledge perspective), a model enables the components of a complex phenomenon to be brought together in one understandable whole (Macionis and Ken 2008). The terms good, middle range, and substantive model (Macionis and Ken 2008) are used to describe the scale of what is being proposed, although exactly what constitutes a good model has been a subject of debate (Berberoglu 2005, Baert and Carreira 2005, Macionis and Ken 2008). According to Baert and Carreira (2005), such debate has arisen due to increasing interest in the area of model building.

2.2 Management and Organisations

2.2.1 Theories of Management and Organisations

According to Hatch (2002), some of the earliest research on organisational environments was built upon the observation that organisations differ considerably depending on whether they operate in a stable or rapidly changing environment. In stable environments, organisations are characterised by strict and clear lines of responsibility whilst in rapidly changing environments, organisations require flexibility and employees are not subject to

the same rigorous control. This notion tallies with contingency theory (Cade2002) discussed in section 2.1.2. Contingency theory is used by many organisational theorists[23] (see for example William 2001, Hatch 2002, Cade 2002, Scott 2007 and Baron and Greenberg 2008) to provide a framework for deciding the most appropriate strategy for the organisation, and the importance of adopting the correct posture is highlighted by Scott (2007) who notes that scientific studies show that organisations which are too set in their ways (having too many rules and too much central control) ultimately cease to exist; and organisations which are too loose in their ways (have few rules and everyone looks after himself with little interest in others) also do not survive for long.

Baron and Greenberg (2008) indicate that managements[24] of unstable firms seem reluctant to attribute poor performance to uncontrollable environmental events and instead, demonstrate what is called illusions of control by manipulating the words they use to describe the outcome of events. This has important implications for the way managers behave when times are difficult and when the need for sound judgement and good management is paramount.

Drawing on the work of Petit (1967), Tompkins (2005) argues that there are different types of managers who may be differentiated according to task, viewpoint, techniques, time horizon and decision making strategy. He explains a behavioural theory of management as

[23] Organisational theory is the study and application of knowledge to how people - as individuals and as groups - act within organisations (Hatch 2002).

[24] Management in business areas and organisational activities is the act of getting people together to accomplish desired goals and objectives (Robbins 2004).

the actions that management takes in dealing with the firm's primary needs for uncertainty avoidance based upon the organisation's environment (Tompkins 2005).

The UAE commercial banks operate in a multi-cultural fast moving and rapidly changing environment, and according to the above analysis will need to continuously adapt to survive. Fundamental to this, generally speaking, will be the role of management in deciding upon the most appropriate strategy. The importance of managers as a distinctive occupational category has long been recognised by a number of scholars (see for example Taylor 1911, Fayol 1949, Carter 2004, Tompkins 2005 and Gomez and Luis 2008).

Carter (2004) claims that management is a set of individuals distinguished by the activities they perform, and goes on to identify four management perspectives Carter (2004, p. 89):

1. Management functions: the essence of management can be distilled into a number of functions (production, administrative, innovative, and so on), which need to be carried out in all organisations although how they are carried out may differ;
2. Management task characteristics: the tasks that management have to do within the functions are characterised by a number of different features such as being highly interdependent and context dependent;
3. Management roles: managers' jobs can be analysed into a number of interrelated roles related to behaviours and attributed to relative hierarchical positions;
4. Management control: arising from the nature of the relations of productions, management is compelled to create structures of control over the labour force.

Carter (2004) concludes his analysis by proposing that the four perspectives may be viewed as ontological or natural layers of management with different layers exhibiting different rates of change depending on how various contingencies influence a particular layer.

The development of appropriate performance measures is picked up by Woods (2009) who advocates a contingency theory approach to performance measurement since, as the environment becomes more unstable, then performance measures must be sufficiently flexible to reflect resulting discontinuities. He points out that the establishment of performance measurement systems that are wrongly focused or too rigid may precipitate the fall into organisational decline, and the risk performance measurement systems fall within this area (Woods 2009).

2.2.2 The Organisation and Its Environment

The author would contend that Porter's (1985) work on the five forces has been providing a well-established framework from which an organisation can objectively view its environment and the threats and opportunities that may be ahead (see section 2.4.1for details of the five forces). Preparing for an uncertain future is best done by identifying the major events that have already happened and that will have predictable effects in the next decade or two (Drucker 1997). External environmental factors that can play an important role in determining strategy, and questions such as 'what external forces are shaping competition?' are viewed by El-Dyasty (2004) as helping to stake out the future.

Environmental uncertainty has been well researched over the last few years (see for example Dean and Shanley 2000, Mulcaster 2009) with the dominant focus being on internal uncertainty reduction strategies or a focus on acquiring knowledge about the operation of the organisation. External uncertainty reduction strategies are described by Dean and Shanley (2000) as a means of acquiring knowledge about the environment and, where possible and desirable, creating more uncertainty for others in order to try and gain competitive advantage[25]. Acquiring such knowledge is often done by units within the organisation, which perform staff functions such as market research, or it may be integrated into the responsibilities of those who operate in the external environment, such as salesmen (Mulcaster 2009).

The UAE commercial banks are currently subject to much environmental uncertainty in the area of risk. This is being driven by a number of factors including the regulatory situation (Basel II), the Financial Crisis, Dubai Crisis and the move for a Gulf Cooperation Council (GCC) single currency. These factors will be thoroughly examined in this literature review (section2.4.1).

[25] Competitive advantage theory suggests that states and businesses should pursue policies that create high-quality goods to sell at high prices in the market. Emphasis is on productivity growth as the focus of national strategies. The other theory, comparative advantage can lead countries to specialise in exporting primary goods and raw materials that trap countries in low-wage economies due to terms of trade. Competitive advantage attempts to correct for this issue by stressing maximising scale economies in goods and services that garner premium prices (Porter 1985).

2.2.3 Decision Making in the Organisation

Based on a study of Chief Executive Officers' career path and the processes and problems they encounter when making decisions, Tedlow and Purrington (2003) point out that it is imperative to realise that the perfect decision making environment exists only in the minds of theorists. They conclude that even successful companies have not yet solved some of the important problems of management.

The work of Simon (1997), cited by Brooks (2002, p. 175) provides a four phase decision-making model, covering:

1. Intelligence activity – searching the environment for conditions calling for decisions;
2. Design activity – inventing, developing and analysing possible courses of action;
3. Choice activity – selecting a particular course of action;
4. Review activity – assessing past choices.

Lurie (2004) expands upon the last activity and describes it as an implementation phase where the action plan from the choice activity is implemented. Lurie (2004, p. 473) goes on to explore the choice process in some detail and comes up with five types used by decision makers:

1. Historical: the solution would be drawn from the practice of others and would involve the decision maker selecting a procedure which is known to work;
2. Off-the-shelf: the solution is drawn from a selection of best ideas collected by the decision maker;

3. Appraisal: the decision maker begins with an idea that has an unknown value and seeks to implement it rationally and top down;
4. Search: the decision maker seeks a new solution but needs help in knowing where to look;
5. Nova: the decision maker seeks to implement a solution which is innovative and aims to challenge the way things are being done in the organisation.

Simon's (1997) model, as pointed out by Brooks (2002) is, however, not without its critics. Sloan (2008) argues that the framework is a serious obstacle for the evolution of Decision Support Systems (DSS) and practice, arguing that different types of DSS could emerge from the adoption of alternative perspectives of human decision-making. DSS aims to extend methodologies and techniques developed in different research areas and to combine them into a new form of computer-based systems able to support and enhance managerial decision-making (Sloan 2008). Such systems may be developed to (Sloan 2008, p. 123):

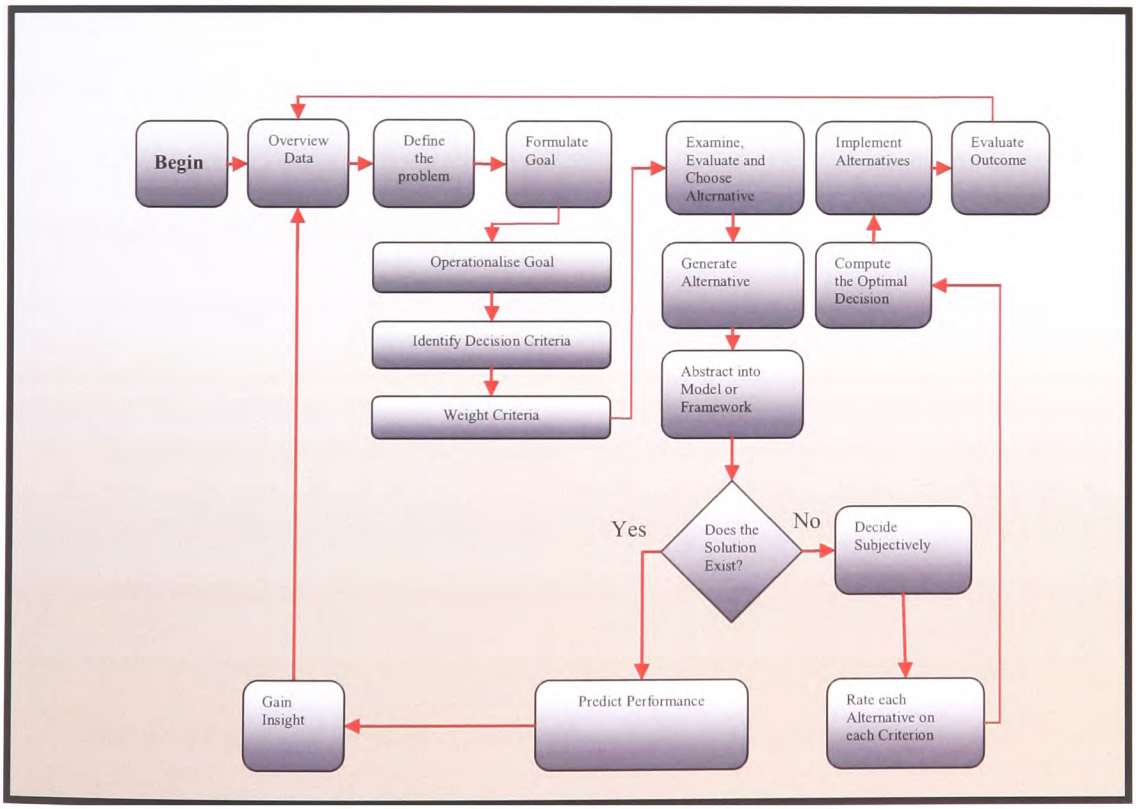
- Facilitate the structuring of a decision so that the analytical tools, possibly several in combination, can be used in generating solutions;
- Facilitate the use of the analytical tools and bring them together through a structuring process;
- Facilitate the manipulation, retrieval and display of data.

Despite the growing interest in DSS, Palocsay (2008) notes that the subjectivity cannot be removed from the decision-making processes, and that there is no substitute for intuition, experience and judgement when it comes to making decisions. Palocsay (2008) goes on to

point out that people do not work mechanically in their business nature; they work by experience, instinct and analysis.

Robbins and Timothy (2008) develop a decision making model starting with the process of realising a problem, establishing and evaluating planning criteria, creating alternatives, implementing alternatives, and monitoring progress of the alternatives. They claim that the model is central in the development of modern DSS being a process for making logically sound decisions by following an orderly path from problem identification through to solution. Figure 4 illustrates the model.

Figure 4: Decision Making Model



Source: Robbins and Timothy (2008)

Robbins and Timothy (2008) argue that their model is suited for structuring a DSS because the generic aspect of the model allows decision makers to concentrate on actions specific for particular phases of the decision-making processes, and its analytical feature contributes to the decomposition of the decision problem between its components.

From operational risk mitigation perspective, a risk management support system is based on the DSS domain. As will be discussed in section 2.4.3, Aref (2009) in his review of information technology for risk management highlights that many financial institutes have risk management support systems already in place whereas many others have already started the deployment process.

Henri and Journeault (2009) provide an analysis of some decision-making models and propose a contingency theory of decision-making which relates the situation facing the decision-maker to the model to be used. Their analysis looks at the models by functional area, by process and by level (in the organisation). They make a number of specific recommendations some of which are important in the context of operational risk:

- Theorists must carefully study the real world of decision-making: the focus should be on understanding the application of the model in the field where dynamic factors can be assessed in the context of the model;
- Decision models must encompass the whole decision-making process: the need to look at risk mitigation in the context of the wider management of risk and;

- Models must deal particularly with dynamic factors and multiple goals: the need is for open-system models of decision-making which recognise conflicting goals, limited data, timing difficulties, possible interruptions, delays to implementation and of the factoring of larger decisions into smaller ones.

Mukherjee (2008) provides an analysis on decision-makers and their behavioural attitude to risk when making a decision. He notes that decision-makers have a strong tendency to consider problems as unique, and the natural way to think about a problem is to exploit all one knows about it (experience), whilst paying special attention to its unique features. He also finds that people also exaggerate their control over events and the importance of the skills and resources they possess in ensuring desirable outcomes from the decision; leading to more decisions being taken without fully appreciating the risks involved. In looking at whether organisations provide effective controls against the optimistic bias of individual executives, he observes that a rational organisation would want to base its decisions on unbiased odds but that arrogance or optimism can lead to mistakes in decision-making that can cost the organisation dearly. Evidence to support this view comes from Asif (2010) who suggests that managers can spend a substantial part of their time dealing with consequences of bad decisions.

Asif (2010) indicates that some interesting issues arise for banks in the context of operational risk mitigation. A consistent approach to operational risk mitigation (decision making) is arguably required if managements are to act rationally when faced with

operational risk problems. The challenge facing managements is to articulate and spread their approach as an integral part of the ORM control strategy.

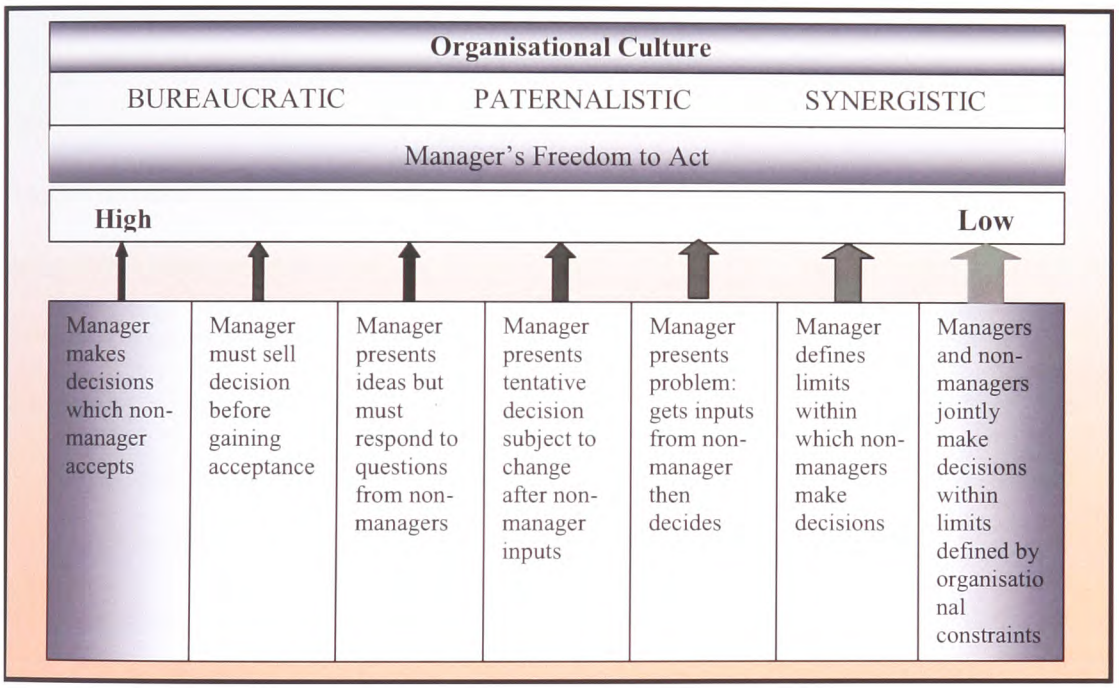
2.2.4 Barriers to Decision Making: the Theory of Bounded Rationality

The literature review reveals that decision-making is one of the toughest as well as one of the riskiest jobs of any executive (see for example Hammond et al. 1998, Cash and William 2002, Fioretti 2008, Henri and Journeault 2009). Fioretti (2008) points to a number of psychological traps that are particularly likely to undermine business decisions: the anchoring trap, the status-quo trap, the confirming-evidence trap, the framing trap and the estimating and forecasting traps. Many of these traps can work in isolation or in concert. His argument supports the view of Martin et al. (2004) who discuss Simon's (1972) theory of bounded rationality which locates the constraints of decision-making mainly in the decision maker. The theory of bounded rationality postulates that in decision making, the rationality of individuals is mainly limited by the cognitive limitations of their minds. Also, the information they have and the finite amount of time they have to make decisions are limiting factors (Simon 1972).

The literature review found substantial work on the 'games' that decision-makers play (see for example Brindle 1999, Kelly 2003, Sanfey 2007). In his review of the cognitive decision processes Sanfey (2007) identifies some games that managers play, such as misuse of analogy, framing and rationality, and argues that whilst we cannot control human nature at the decision-making table, we can learn to be more adept at the games which are played every day.

Citing Basi (1998), another aspect of decision-making that is noted in the literature by McKinnon (2003) is based on the position of the decision-maker in the organisation and the organisational culture. McKinnon (2003) provides an analysis of decision-making styles vis-à-vis organisation cultures and illustrates manager's freedom to act on a decision-making continuum, as illustrated in Figure 5.

Figure 5: Organisational Culture and Manager Decision-making Ability



Source: Adapted from McKinnon (2003)

As can be seen from the diagram, the degrees of freedom available to the manager vary considerably depending upon the type of organisational culture that exists. Finally, Graham

(2008) advocates that the risk maturity of the organisation is seen as a possible constraint against selecting a particular course of action.

The discussion in this section identifies some of the barriers or constraints that occur when decision-making has to take place in the organisation, and illustrates some of the complexities involved in the decision-making process, all of which have implications for the way an operational risk mitigation decision is taken.

2.2.5 Implications for Operational Risk Management

There is evidence to indicate that the UAE commercial banks are facing a changing external environment and that management will need to keep abreast of the changes that are occurring and the operational risks that they may bring. Part of the management process entails looking ahead, planning for expected and unexpected outcomes, organising adequate resources, and controlling the work done. The operational risks associated with the future strategic intent of the bank in this turbulent environment, will require effective mitigation strategies. Management behaviour in dealing with these risks must take account of any delusions of control that may exist, and the development of appropriate performance measurement systems to monitor operational risks will assume increasing importance.

Operational risk mitigation involves making a decision and, as the analysis in this section has shown, this can involve a complicated set of processes contingent upon the nature of the risk. The complexity and subjectivity of the process provide illustrations of some of the constraints that put pressure on managers when the choice has to be made about what to do.

The implication is that there should be a drive towards a more uniform and structured approach to the risk mitigation process, taking into account the organisational culture and the freedom of managers to act.

2.2.6 Summary

This section has provided some theoretical propositions relating to organisations, management within organisation, how the organisation copes with environmental factors and decision-making. The emphasis within this section has been to provide a theoretical underpinning for the research, and to place the research area, operational risk mitigation, in the wider body of knowledge concerning management and organisations. The review highlighted how contingency theory and bounded rationality theory can play an important part in both the organisational structure and the decision-making process. The behavioural aspects of management and the internal environment in which it has to operate also feature in the day-to-day decisions that managers have to make. The section concluded with a review of the implications for ORM.

2.3 Risk Management

2.3.1 The Concept of Risk and Risk Management

> "...managers in the past did not want to deal with information of historical nature, but today, the emphasis is on identifying a potential problem and taking action before it happens."

This quote from one of the Risk Managers interviewed appears to capture the essence of what proactive, as opposed to reactive risk management (Douglas 2009) is all about: identifying a potential problem (risk) and taking action (mitigation) before it happens. This is a view shared by Masli and Peters (2009) and Hopkin (2010) who describe the activity of risk management as being the embodiment of the old proverb: prevention is better than cure.

It is likely that most people's understanding of the word risk would trigger the thought of something that could go wrong. A point emphasised by the Oxford English Dictionary definition of risk, that is; "the possibility of incurring misfortune or loss." This negative definition of risk, however, ignores the expected benefits of rewards that can accrue from taking risks and management has plenty of opportunities to take speculative risks in areas such as the investment function, where the decision to invest can subsequently yield losses as well as gains. Equally, a failed business acquisition, a missed opportunity to enhance performance, or the failure to move into a new business area are as much a risk as the possibility of a control failure (Branger and Schlag 2004).

The concept of risk was normally associated with insurance (Branger and Schlag 2004), a point emphasised in the past by describing the Risk Manager's role in the organisation as being involved with the technical aspects of insurance (Robert1999). In current organisational terms, risk and how it is managed have taken a much broader dimension. Hence, the assessment of risk and the development of corporate strategy should now go hand in hand, as outlined by Alexander and Sheedy (2005). This change in risk

management paradigm is illustrated by Alexander and Sheedy (2005), who describe it as reinventing risk management, as per Table 1.

Table 1: Reinventing Risk Management

Old Paradigm	New Paradigm
Functional approach, limited to the risk management department	Process approach transcending functions and divisions
Insurance perspective	Business perspective
Risk Manager	Risk process manager
Senior Management support	Board and Senior Management support and involvement
Insurance jargon understood by a few	Common risk language understood by the boardroom downwards

Source: Adapted from Alexander and Sheedy (2005)

The table identifies how risk management has broadened to cover all aspects of the business as well as illustrating how Senior Management understanding and involvement is essential in establishing the risk management culture.

Dionne (2005) notes that the general concept of risk is the chance, in quantitative terms, of a hazard occurring. It, therefore, combines a probabilistic measure of the occurrence of an event with the measure of the consequence of that event.

According to Caplan (2004) risk is a dominant feature of society. The business of estimating and addressing risk is complex and controversial and has become an industry with many competing specialists, a view confirmed by Ishmael and Stacy-Marie (2005).

Lam (2006, p.12) points out that the discipline of risk management is well advanced in sectors outside of the financial services, and identifies a number of different experiences of risk management:

- The fundamental risk assessment processes are subjective and risk cannot, therefore, be unambiguously measured in objective terms;
- The actions of people cannot be predicted with certainty, and individual action in particular, cannot be pre-specified and reduced to a simple numerical representation;
- In the case of extreme events, data is likely to be in short supply; making it extremely difficult to obtain a realistic, quantitative appraisal given the high level of uncertainty;
- For a dynamic organisation operating in a dynamic global economy the past is not necessarily a good predictor of the future.

These experiences illustrate the complexity of risk management, and some of the difficulties associated with quantifying risk exposures.

The growing interest in risk and risk management is evidenced by the increasing attention being shown by the quality Journals about the subject such as: Risk Magazine, Journal of Operational Risk, Operational Risk and Regulation, Risk.net, OpRisk Compliance and Regulation. These Journals are monthly and quarterly periodicals specialising in all aspects of risk with particular emphasis on operational risk. They draw on the collective

experience of practitioners and academics alike and provide a comprehensive overview of the important concepts of risk management. Given such increasing interest in risk management, it begs the question: Why should organisations manage risk? Hopkin (2010) argues that good management is risk management, because it is inevitable for all managements. The Public Risk Management Association (2010, p.45) furnishes five reasons why it believes firms should manage risk:

1. Risk management can be used to align interests of management with those of the owners of the company;
2. Risk management can be used to improve cash dividends;
3. Risk management can be used to encourage and protect from adverse events;
4. Risk management can be used to assist firms in developing financial plans and funding programmes;
5. Risk management can reduce the costs of financial distress and bankruptcy.

A number of these issues are to do with managing cash flows, for example, the stabilisation of cash dividend payments, and both managing cash and managing risk are seen as essential for survival (Gewei 2008). Sabato (2009) goes as far as saying that risk management programmes should have an overarching goal of enhancing cash flows, which in turn should lead to improved firm performance.

2.3.2 Risk Management Framework

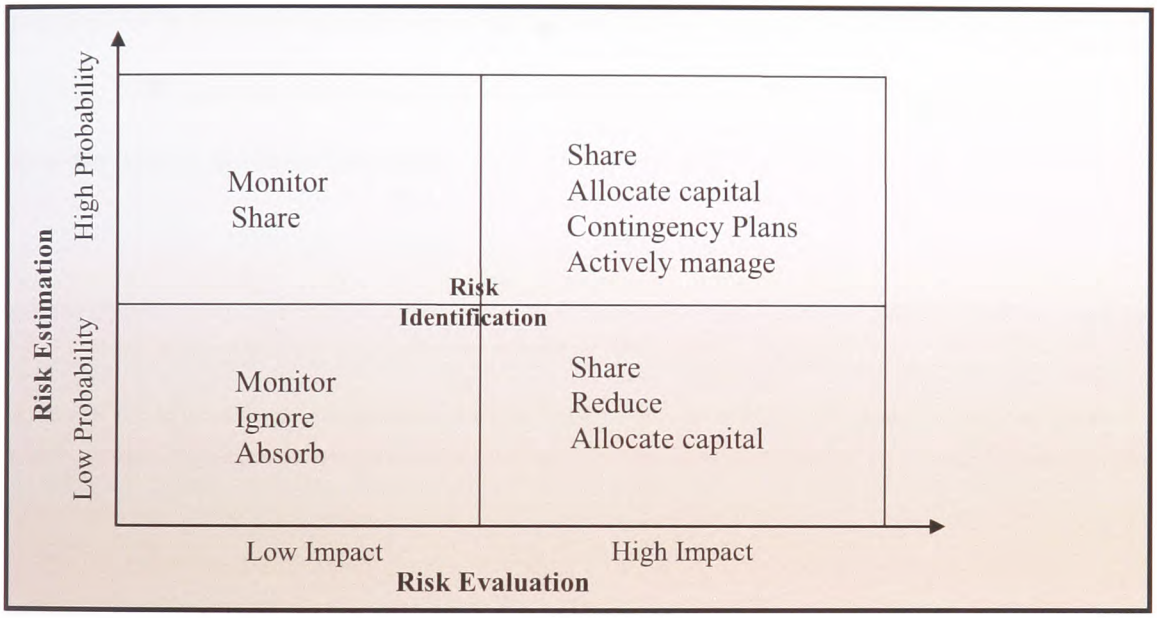
BCBS published its 272 page comprehensive revised framework: *"International Convergence of Capital Measurement and Capital Standards"* in the year 2006. The framework primarily focused on recommendations on banking laws and regulations. Its purpose is to create an international standard that banking regulators can use when creating regulations about capital adequacy to guard against the types of financial and operational risks banks face (Basel II). The framework is currently used by the majority of countries in the world (Moosa 2007). The literature review revealed that besides BCBS, a multitude of authors addressed risk management as a contemporary topic and reiterated its extreme importance (see for example Sadgrove 1996, Scandizo 2005, Hull 2006, Gewei 2008 and Sabato 2009).

In considering how to manage risk, Andersen and Torben (2005) provide a framework based on three components and focused on negative connotation of risk: the exposure to loss, the chance of loss and the magnitude of loss. The components of loss are described by Venkataraman (2006) as being a threat (a disaster that can lead to a loss of resources), which leads to an event (a loss of resource for a definite time period). Venkataraman (2006) argues that to manage risk, you need to reduce one or more components. This description could involve building complex models based on previous risk exposures within the organisation, assuming one is able to capture the data. (Gustafsson 2007).

A number of authors (see for example White 1995, Parker 2005, Millo and MacKenzie 2007, Jason 2009) summarise the principal approach to risk management as outlined in section 1.1.2. This approach can then be applied equally to all types of risk exposure within

a company (Parker 2005) and is summarised in the model shown earlier in Figure 1. The model involves a systematic approach to risk identification, estimation, evaluation and mitigation. Figure 6 draws on the work of Millo and MacKenzie (2007) and illustrates how risks can be categorised into one of four quadrants, depending on how the probability (risk estimation) and impact (risk evaluation) of the risk are assessed.

Figure 6: Risk Management Framework with Mitigation Strategies



Source: Millo and MacKenzie (2007)

In addition, a whole body of literature has been developed on frameworks for managing project and enterprise risks (Lam 2005). COSO (2004) develops an enterprise risk management integrated framework; Bena (2006) examines risk classification methodologies for the information technology (IT) projects; Virine and Trumper (2007)

look at the tools used in managing project risks; Kenneth (2009) illustrates a system for prioritising project risks, and tracking the progress of risk mitigation.

The reader will note that these frameworks are built around proactive risk management, i.e. trying to prevent something from happening rather than dealing with something that has happened (reactive management). Other methods for proactively managing risks are discussed by Alexander and Gordon (2008) who discuss techniques for benchmarking risk management in the organisation with suggestions on how it can be improved. James and Roberts (2009) maintain that organisations should predict and handle risk crises promptly since they do not improve with time.

2.3.3 Risk Perceptions and Decision Making: Prospects Theory

Dake (1990) argues that our attitudes towards risk vary according to what has happened to us, what we expect, what we feel and what we care about. In other words, our perceptions of risk are selective and change as our social and business lives change. He explains five theories of risk perception as follows Dake (1990, p. 41):

1. Knowledge theory: people perceive technologies to be dangerous because they are not familiar with them;
2. Personality theory: some individuals love risk-taking so they may take many risks, while others are risk averse and seek to avoid as many risks as they can;
3. Economic theory: the rich are more willing to take risks stemming from technology because they benefit more and are somehow shielded from adverse consequences;
4. Political theory: people view the controversies over risk as struggles over interests;

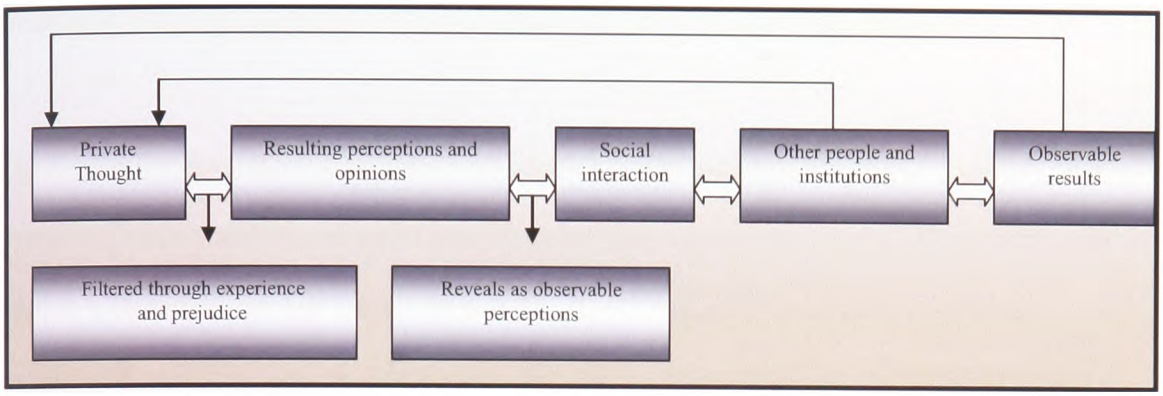
5. Cultural theory: adherents of hierarchy perceive acts of social deviance (risk) to be dangerous because such behaviour may disturb their preferred subordinate form of social relations.

Dake (1990) goes on to conclude that people perceive a variety of risks in a manner that supports their way of life and suggest that risk communication programmes might profitably be used to focus on the underlying causes of risk perception rather than only on the possible harms. This point on risk communication is picked up by a number of authors (Recchia 1999, Ragnar 2004, Nielson et al. 2005). Nielson et al. (2005) discuss why risk communication, or the science of understanding scientific and technological risk and how it is communicated, have become so important, and why risk communication programmes will only be successful if they raise the level of understanding of relevant issues or actions, and satisfy those involved that they are adequately informed within the limits of available knowledge.

Biais (2006) notes that one of the reasons why a risk analysis may not be carried out in a project is because there is a perception that the risks are not sufficiently great or are too poorly understood to justify analysis, and a perception that the risks will in any case be borne by the parties.

The interplay of the variables that influence how people formulate their perceptions of risk has been studied by Otway and Thomas (2006) and their model is shown in Figure 7.

Figure 7: Risk Perception Formulation Model



Source: Otway and Thomas (2006)

Risk perceptions are important in a business decision-making context; because a substantial part of the literature dealing with risky choice behaviour assumed that decision makers are risk averse (Bigoni and Frid 2008). Prospect theory, however, developed by Kahenman and Tversky (1979) indicates that when managers anticipate negative changes in wealth, they display risk seeking behaviour, but when anticipating positive changes in wealth, they exhibit risk averse behaviour. Prospect theory is a theory that describes decisions between alternatives that involve risk, with uncertain outcomes. The model is descriptive and tries to model real-life choices, rather than optimal decisions (Kahenman and Tversky 1979). Adams (1998) describes such behaviour as being the balancing act between risk and reward.

Recent advances in behavioural decision theory have also confirmed that most individuals exhibit a mixture of risk seeking and risk averse behaviour (Bigoni and Frid 2008), a view supported by McDermott et al. (2008) who develop a behavioural agency model of risk-

taking which suggests that managers' risk-taking behaviours vary according to the type of monitoring they are subjected to by the principals of the business (shareholders).

Other research into risk-taking behaviour (Taylor 2008) highlights how the factors perceived control and the nature of the risk information available have an important role to play in influencing the risk-taking decision managers make. Information can play an important part in the decision-making process about a risk, and Agarwal (2008) notes that insufficient attention has been given to the information requirement of risk management decisions. Michael and Ebert (2009) suggest that risk management decisions can be significantly improved when managers are aware of the full range of controls at their disposal.

The practical realities of decision making in an operational environment are investigated by Sloan (2008) who supports the use of DSS for interactive real-time risk management where the decision maker is able to analyse risks and make decisions in real time during unexpected disruptions in the operations (see section 2.2.3 for a discussion on DSS systems).

It should be apparent from the previous discussions that the aspect of risk perception is important in determining the decision made by the manager. There does not appear to be a 'one size fits all' model because the number of different variables at play is large and diverse. Woods (2009), in investigating a contingency model of strategic risk-taking, identifies a number of key variables that he considers affect the risk decision. For example,

self-confidence, knowledge, biases, and performance of the decision maker are important, whilst in the environmental area, the economy, government regulations, technological change and cultural values need to be addressed, too.

2.3.4 Focus on Operational Risk

2.3.4.1 Reviewing the Definition of Operational Risk

As discussed in section 1.1.1, BCBS published its second Capital Accord to address operational risk: *"International Convergence of Capital Measurement and Capital Standards"* in 2004 (BCBS 2004), and a revised edition in 2006 (Basel II). A survey made by the author revealed that Basel II incorporated the phrase 'operational risk' on 145 occasions. The author would contend that such emphasis could be interpreted as an indication of the importance of operational risk in the banking sector.

Basel (2001, p. 32) defines operational risk as *"The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or external events."* Basel II upgrades the definition to include legal risk but exclude strategic and reputational risks (section 1.1.3), thus;

> *"Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk"* (Basel II, p. 140).

The origins of this definition of operational risk are derived from the major operational risk survey undertaken by the British Banking Association and Price Waterhouse Coopers (BBA 1999a). Whilst it may be that the latter definition became universally accepted, the

literature evidences a large number of definitions were formulated to describe the term 'operational risk.' The following is a cross-section of some of the definitions:

> "*Operational Risk is the risk that improper operation of trade processing or management system will result in financial loss. Operational risk encompasses the risk of loss due to the breakdown in controls within the firm including, but not limited to, unidentified limit excesses, unauthorised trading, fraud in trading or in back office functions including inadequate books and records and a lack of basic internal accounting controls, inexperienced personnel, and unstable and easily accessed systems*" Oldfield and Santamero (1997, p. 33).

> "*Operational Risk is the risk of loss resulting from breakdown in administrative procedures and controls or any aspect of operating procedures*" Treasury Management Association of Canada (1998, p. 11).

> "*Operational Risk is the difference between the inherent risk of an activity and the hedges used to mitigate the risk*" Senior (1999, p. 24).

> "*Operational Risk is the risk that deficiencies in information systems or internal controls will result in unexpected loss. The risk is associated with human error, systems failure and inadequate procedures and controls.* " This was a sample definition from one bank.

> "*Operational Risk is the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or external events* " BBA (1999a, p. 17). This definition was adapted by Basel II to produce its definition version of operational risk.

> "*Operational risk is the problems associated with accurately processing, settling, and taking or making delivery on trades in exchange for cash. It also arises in record keeping, computing correct payment amounts, processing system failures, and complying with various regulations.* " Currie (2004, p.14)

> "*Operational Risk is the risk arising from execution of a company's business functions due to people, systems and processes through which a company operates. It includes fraud, legal, physical and environmental risks* " OCC (2005, p. 18).

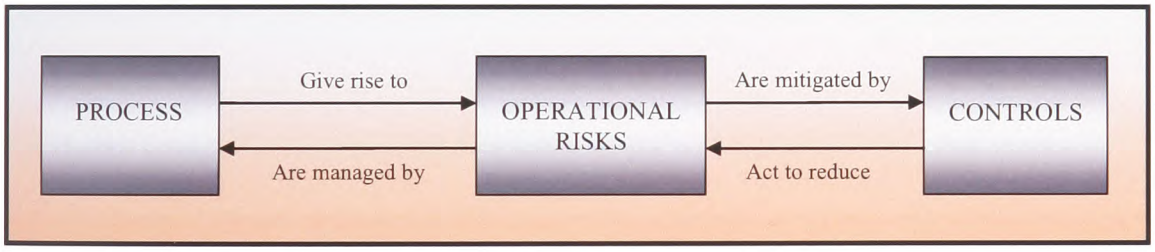
The field interviews in the selected UAE commercial banks revealed that Basel II definition is the one accepted amongst most of the UAE commercial banks as the workable definition; with minor variations in some cases to accommodate specific bank requirements. This phenomenon will be discussed during the analysis of the study findings (Chapter 4).

Apart from the second definition which appears to be very specific and that of Senior (1999) which appears to leave open many questions such as 'what is an activity?' the others appear to have a theme: a loss resulting from breakdown (failure/deficiency) in the internal controls (systems/procedures). This breakdown can occur for a variety of reasons some of which are quoted above: inexperienced employees, unauthorised trading and fraud. Equally, a breakdown can occur because there is no control (or controls) in place to reduce the possibility of the risk occurring. Only one of the definitions (Treasury Management Association of Canada) places a boundary around the definition by linking the breakdowns to operating (as opposed to strategic) procedures which give rise to operational risk. It is probably safe to assume that this boundary is implied in all the others, although some definitions appear to have a narrower focus than the others.

The common theme referred above in the definitions indicates that a loss will occur when an operational risk event manifests itself. This happens, for example, when there is a breakdown in the control systems, which are designed to mitigate the risk. This establishes

a link between a risk and a control[26], i.e. a risk is mitigated by a control (or a series of controls), and a control acts to reduce the probability of a risk occurring. A further common feature of the definitions is that risk resides within the business/process/procedures/systems or, putting it more concisely, the internal control environment that exists within a company. This is pointed out in Basel II which notes that operational risk is principally addressed through a firm's internal control framework. Continuing with this logic, it can be seen that the internal control framework (or the processes within it) gives rise to (operational) risks which are in turn mitigated by controls. Diagrammatically this can be represented as shown in Figure 8:

Figure 8: The Process-Operational Risk-Control Triode



Source: Developed by the author

Whilst this simple diagram may draw together the common components of operational risk and be intuitively easy to understand, it does not necessarily illustrate the potential for loss arising from external as opposed to internal events. The author, however; offers it as a pictorial way of describing what is meant by operational risk from an internal perspective.

[26] The term control is used to describe any action which serves to mitigate a risk. This could include but is not limited to internal accounting controls, risk management policies and any other form of management control (Merchant 2002 and Spira and Page (2003).

2.3.4.2 Operational Risk Sources

According to the BBA (1999a, p. 22), banks acategorise operational risk sources into a number of different areas to help managers understand what the definition encompasses. Such areas include:

1. System failure and error.
2. Transaction processing error.
3. Business interruptions.
4. Internal and external criminal act.
5. Personnel errors.

However, different banks use different categories and sub-categories, suggesting that operating procedures and hence operational risk sources are interpreted differently by different banks. On the other hand, Basel (2006, p.257) classifies operational risk sources, and hence operational risk event types in more detail, as follows:

1. Internal Fraud - misappropriation of assets, tax evasion, intentional mismarking of positions and bribery.
2. External Fraud- theft of information, hacking damage, third-party theft and forgery.
3. Employment Practices and Workplace Safety - discrimination, worker compensation and employee health and safety.
4. Clients, Products and Business Practice- market manipulation, antitrust, improper trade, product defects, fiduciary breaches and account churning.
5. Damage to Physical Assets - natural disasters, terrorism and vandalism.

6. Business Disruption and Systems Failures - utility disruptions, software failures and hardware failures.
7. Execution, Delivery and Process Management - data entry errors, accounting errors, failed mandatory reporting and negligent loss of client assets.

In its June 2010 operational risk report, which contains a high-level overview of the global operational risk loss database and the high level trends in operational risk losses, ORX Association (2010, p. 32) classifies operational risk sources slightly differently, thus:

1. Internal fraud.
2. External fraud.
3. Employment practices and workplace safety.
4. Clients, products and business practices.
5. Disasters and public safety.
6. Technology and infrastructure failures.
7. Execution, delivery and process management.
8. Malicious damage.

Further, the report reflects operational risk event severity and frequency on the various business lines for a time horizon of one year (2009): corporate finance, trading and sales, commercial banking, clearing, agency services, asset management, retail brokerage, private banking, corporate items and multiple lines.

Analysis of the report (ORX Association 2010) data reveals that the top three event types that account for more than 85% of the number of total operational risk events - in descending order; with the maximum severity and frequency are:

1. Fraud – internal and external;
2. Execution, delivery and process management;
3. Clients, products and business practices.

The author would contend that banks need to prioritise the management of these types of operational risk, with special emphasis on fraud that will be discussed in more detail in the next section. Another finding in the report is that commercial banking is incurring the maximum number of operational risk events, with the maximum severity and frequency, totaling losses amounting to billions of dollars per year (ORX Association 2010). This gives more impetus to the research, and demonstrates that the selection of operational risk mitigation as an area of research in the UAE commercial banking industry is extremely important and intuitively appealing and challenging to the author.

2.3.4.2.1 Fraud: General Deterrence Theory

Internal and external fraud are two major sources of operational risk out of seven, as classified by Basel II, that every organisation faces. ORX Association (2010) points out that banks are vulnerable to the impact of fraud. The large scale losses that banks have suffered bear witness to this; perhaps the most famous being BCCI which resulted in the complete collapse of the bank. Other recent examples of severe losses incurred due to fraud

are the Madoff[27] (Clauss and Roncalli 2009) and the Société Générale cases. Carpenter (2007) discusses certain types of fraud to which banks are particularly vulnerable, including card[28] fraud, phantom cash withdrawals, internet fraud and money laundering. Money laundering, or the attempt by criminals to legitimise the proceeds of crime by placing it into legitimate accounts is one area of concern for all banks where they work together to combat this type of fraud (Carpenter 2007).

Computer Crime Research Centre (2005) discusses another type of fraud that hits banks, that is of crime in cyberspace, and illustrates, in particular the jurisdictional issues that can arise due to the complexities of establishing where the event took place, and having governments with harmonised computer crime laws (Computer Crime Research Centre 2005). Wikimedia Foundation (2010) lists more than twenty banking fraud scenarios. Fraud against banks and the methods used to bring the perpetrators to justice are discussed by Green and Reinstein (2004). They point out the complexities that can be involved with bank fraud and the administrative steps that need to be taken. All of these points illustrate the need to ensure that adequate control procedures are in place to guard against the threat of fraud risk and the impact that it may have on the bank both in financial and reputational terms.

Theoretical propositions concerning the effectiveness of counter measures taken to prevent fraud acts include the General Deterrence theory (Straub and Welke 1998). This theory

[27] For detailed analysis of operational risks in the Madoff case see Clauss & Roncalli (2009).

[28] The term card embraces credit and debit cards, charge cards, and all similar instruments.

points that individuals with an instrumental intent to commit antisocial acts can be dissuaded by the administration of strong disincentives and sanctions relevant to these acts (Straub and Welke 1998).

2.3.4.3 The Increasing Emphasis on Operational Risk Management

> "It is difficult for banks to understand the extent of the risks they are assuming at any moment. Their ability to understand risk often lags seriously behind their urgent need to do so."

The above quote by one of the Risk Managers interviewed in this research illustrates a growing problem for banks, how to ensure that the risks they manage today are the ones that could affect their performance tomorrow. How well do banks understand operational risks and the impact that they have on the business? Netter and Poulsen (2003) consider that the re-engineering of the business in recent years has forced bank management to look afresh at the challenges of operational risk.

BCBS (2003) issued its revised fifty-one article document "*Sound Practices for the Management and Supervision of Operational Risk.*" Special emphasis was placed on four areas of operational risk (BCBS 2003, p.21):

1. Role of Supervisors: Banking supervisors should require that all banks, regardless of size, have an effective framework in place to identify, assess, monitor and mitigate material operational risks as part of an overall approach to risk management.

2. Developing an Appropriate Operational Risk Management Environment: The Board should be aware of the major aspects of the bank's operational risks as a distinct risk category that should be managed, and it should approve and periodically review the bank's ORM framework.
3. Risk Management: Banks should identify, monitor, assess and mitigate the operational risks inherent in all material products, activities, processes and systems. Banks should also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risks inherent in them are subject to adequate assessment procedures.
4. Role of Disclosure: Banks should make sufficient public disclosure to allow market participants to assess their approach to ORM.

Moosa (2007b) points out that a new impetus driven by a number of factors has taken shape in ORM. He identifies information technology, business climate, outsourcing, globalisation and regulation. The following discussion demonstrates these factors in more detail:

- Information Technology: Stoneburner and Feringa (2004) illustrate how the rapid development in IT provides the platform from which financial services companies can provide new rapid and enhanced services, the so called online banking[29], to their customers. The reduction in time and transaction costs brought about by these developments has seen new entrants in the UAE banking market. This is a dual-

[29] Online banking (or Internet banking) allows customers to conduct financial transactions on a secure website operated by their commercial or virtual bank.

edged sword in ORM since it requires new processes to deal with the new technologies and new strategies to deal with the instigated operational risks.

- Business Climate: Sandra and Strahan (2004) argue that informed customers, new entrants and financial innovations are the main driving forces that are leading to increased competitive pressures and a greater need to manage operational risk. They also discuss the current climate of rapid change and how it is, for example, reducing decision-making timeframes and making people less aware of unusual events. In such an environment ORM should be an ongoing, rather than a static process.
- Outsourcing: the trend towards outsourcing is noted by Shailey (2005) as being important since this type of service implies that operational risk implications need to be considered and understood as part of contractual negotiations. The author would contend that in reverting to outsourcing, banks should not lose their identities; otherwise, outsourcing can instigate additional operational risks that will overload banks with additional burdens.
- Globalisation: there is an increase in risk exposure when a company leaves its home market and ventures into uncharted waters. Whilst companies can reduce the risk through joint ventures and strategic alliances, the balance will be between the cost of the risk (we are going to do this on our own) and the cost of the control (we are going to play safe and share the risk with somebody else) (Franzoni 2008). In his analysis of various risks, Franzoni (2008) notes the increasing trend towards globalisation with its attractiveness to customers. A point re-iterated by Basu and Hung (2009) who emphasise the marketing economies that can be made, but warn about the resulting operational risks. Such studies illustrate how managing

operational risk exposures, requires a global rather than a national mindset (Basel II). The author would contend that banks should think globally and act locally.

- Regulation: Basel II has placed tremendous emphasis on risk management, disclosure and reporting of risk management activities (Avgouleas 2009). Basel II will be discussed in detail in section 2.4.2

On the other hand, banks should expect some benefits to accrue from more proactive ORM Andreas (2010, p. 31) identifies some of the expected gains:

- A measure against financial crises vis-à-vis the current Financial Crisis;
- A quantifiable reduction in losses;
- Better risk mitigation;
- More efficient allocation of capital;
- Risk 'comfort' for Senior Managers;
- Risk 'comfort' for regulators;
- Improved project investment analysis.

This last point is particularly important in large-scale projects where significant risks (high impact) can occur and where there is a greater need for more comprehensive risk frameworks able to capture where and how risks arise (Bamberger 2010).

Gustafsson (2007) points out that as ORM efforts mature, and gain both the support and the confidence of the Board, they will become increasingly valuable to the business. Perceived initially to support regulatory requirements, these efforts can be leveraged and aligned with

the business performance management. To be successful, however, such alignment must be based on a clear vision of the potential benefits.

Gustafsson (2007) goes on to explain that a bank needs to be focused on the regular monitoring of its operational risk profiles and material exposures to operational risk losses with the Board supporting the proactive management of operational risks. Successfully navigating the road from compliance to value creation can be daunting without a roadmap and a clear vision by the Board. By taking a holistic (integrated) approach to ORM an organisation can significantly lower its risk profile and improve responsiveness to risk scenarios leading to strategic and operational benefits (Gustafsson 2007). Bonson and Flores (2008) argue that the bank's ORM should carry out assessments of operational risks, prepare recommendations for operational risk mitigation, analyse new products, and implement a number of tools recommended by BCBS, including: internal and external data loss collection and reporting, key risk indicators (KRI), and control and risk self-assessments. Further, a bank needs to maintain records for all risk management related data: a reusable library of operational risks and their corresponding controls and assessments, results from individual assessments, KRI's, incidents and mitigation plans (Bonson and Flores 2008).

As a result of increasing emphasis that has been placed on ORM, academic research began to develop. Examples of research into theoretical propositions for operational risk in the financial services arena are numerous. Two examples are given below:

- Wahler (2006) examines the relative contributions of prospect theory (see section 2.3.3) and agency theory[30] explanations for specific operational risks and subsequent firm performance in both regulated and non-regulated environments;
- Moosa (2007) critiques the techniques used for operational risk measurement, concluding that they are all flawed, and proposes that financial institutions should focus their attention on using an agency theory framework for managing operational risk.

2.3.4.4 Internal Control

2.3.4.4.1 Internal Control in Organisations: Control and Complexity Theories

Fayol (1949) identifies control as one of five functions of management, the others being planning, organising, commanding and coordinating. By control he means verifying whether everything occurs in conformity with the plans adopted, instructions issued and principles established. An internal control system has been described by Spira and Page (2003, p. 251) as the policies, processes, tasks, behaviours and other aspects of a company that, taken together:

- Facilitate its effective and efficient operation by enabling it to respond appropriately to significant business, operational, financial compliance and other risks to achieving the company's objectives;
- Help ensure the quality of internal and external reporting;

[30] Agency Theory postulates that the firm consists of a group of contracts between the principals, the owners of the economic resources of the firm, the agents, and the managers who use the economic resources (see Sheedy 1999).

- Help ensure compliance with applicable laws and regulations and also with internal policies with respect to the conduct of business.

This description introduces the concept of risk and how the internal control system responds to or manages the risks that the business faces. As such it provides a link between the maintenance of an internal control system and the management of risk.

The development of control theory is traced by Glasser (1990). Control theory is the theory of motivation which contends that behaviour is never caused by a response to an outside stimulus; instead, control theory states that behaviour is guided by what a person wants most at any given time (Glasser 1990). He contends that the executives in an organisation have plenty of guidance to turn to in performing their functions. Specifically, executives can revert to (Glasser 1990, p. 83):

- Knowledge of the control concepts;
- Knowledge of the processes required to control;
- Knowledge of the characteristics of the control system;
- Knowledge of the problems likely to occur when controlling and, therefore, a knowledge of what to guard against;
- A number of control models;
- A framework of principles for effective control.

On the other hand, complexity theory advocates that ordered and chaotic systems differ by the relationship that exists between the system and the agents who act within it. In an

ordered system the level of constraint means that all agent behaviour is limited to the rules of the system. In a chaotic system the agents are unconstrained and susceptible to statistical and other analysis. In a complex adaptive system, the system and the agents co-evolve such that the agents modify the system by their interaction with it (Bailey et al. 1981).

Drawing on the work of Bailey et al. (1981), the design and analysis of internal control systems to help managers is discussed by Rivkin and Siggelkow (2003) who use complexity theory to illustrate how certain regulatory control requirements can impose theoretically unacceptable costs of analysis with respect to internal control requirements. They argue that that a good framework for developing internal control mechanisms would be useful to guide managers on how to design an appropriate system.

A framework at the organisational level can be attributed to Smith (2006) who addresses the organisational control problem from a different perspective by questioning how to achieve good control. According to Smith (2006), good control should mean that an informed person should reasonably be confident that no major unpleasant surprises will occur. His analysis concludes that good control can be achieved by avoiding some behavioural problems (to do with personnel), and by implementing few types of control to protect against the remaining problems. The options available to protect against these remaining problems are (Smith 2006, p. 130):

1. Problem avoidance controls attempt to disallow opportunities for improper behaviour, for example, automation of a procedure avoids human intervention and provides enhanced reliability;

2. Specific action controls attempt to ensure that individuals perform (or do not perform) certain actions that are known to be desirable (or undesirable), for example, segregation of duties helps to ensure that one person cannot perform an improper act;
3. Control of results attempts to ensure that employees are responsible for certain prescribed results, for example, performance measurement systems which provide rewards that help to ensure that objectives are achieved;
4. Control of personnel attempts to place reliance on staff to do what is best for the organisation, for example, sound communication systems help to ensure a consistent message is given and shared beliefs in organisational goals are created.

The Committee of Sponsoring Organisations of the Treadway Commission (COSO) has been notably active in developing an internal control framework that could be used in practice. Their initial framework (COSO 1992) was used as a benchmark to assess and improve internal control systems. It consists of five interrelated components derived from the way management runs a business. According to COSO (1992), these components provide an effective framework for describing and analysing the internal control system implemented in an organisation. The five components are: control environment, risk assessment, control activities, information and communication and monitoring. Following the enactment of Sarbanes-Oxley Act[31], the COSO (2004) enterprise risk management integrated framework emerged. The COSO (2004) framework expands on internal control,

[31] This law (enacted in 2002) extends the long-standing requirement for public companies to maintain systems of internal control, requiring management to certify, and the independent auditor to attest to the effectiveness of those systems (Bumiller 2002).

providing a more robust and extensive focus on the broader subject of enterprise risk management (Dey and Thomas 2005), and is still geared to achieving an entity's objectives.

COSO (2004) points out that at the micro level, an organisation needs to establish its own internal control structure, which reflects the emphasis which the entity's owners, Board and Senior Management place on controls. The main issues that need to be addressed are discussed by Mikes (2008, p. 25) and are summarised in Table 2.

Table 2: Broad Elements of the Internal Control Structure

Area	Examples of elements of internal control
Methods of assigning authority and responsibility	• Delegation of authority • Assignment of responsibility • Documentation of authorisation • Policies on conflict of interest and acceptable business practices
Management's control methods	• Planning and reporting systems • Investigation and communication of variances from planned performance policies to develop and modify systems and control procedures • Investigation and communication of violation of laws and regulations
External influences	• Laws, rules, regulations of regulatory bodies review and follow-up by external parties
Organisational structure	• Management functions • Reporting relationships • Data processing organisations
Management's philosophy and operating style	• Management attitudes and actions towards reporting • Management's approach to taking and monitoring business risks • Management's emphasis on compliance with laws and regulations • Management's emphasis on meeting financial and operating goals
Personnel policies	• Policies regarding hiring, training, evaluating, promoting and compensating employees
Risk Function	• Risk detection • Risk estimation • Risk evaluation • Risk Mitigation • Risk reporting • Risk communication
Audit committee	• Role in communication between the Board and internal/external auditors • Role in overseeing accounting and financial reporting
Internal Audit function	• Authority of Internal Auditors • Reporting relationship • Role in overseeing the internal control

Source: Adapted from Mikes (2008)

IIA (2009) explains the internal control as any action taken by management to enhance the likelihood that established objectives and goals will be achieved. IIA (2009, p. 29) points out that internal control is the result of proper planning, organising and directing by management, and that there are three types of controls:

1. Preventive – to deter undesirable events from occurring;
2. Detective – to detect and correct undesirable events which have occurred;
3. Directive – to cause or encourage a desirable event to occur.

2.3.4.4.2 Internal Control in Banking

Basel (1998b, p. 54) points to the significant losses incurred by several banking organisations and how they could probably have been avoided if the banks have maintained effective internal control systems. Five types of control breakdowns typically seen in problematic bank cases are identified:

1. Lack of adequate management oversight and accountability, and failure to develop a strong control culture within the bank;
2. Inadequate recognition and assessment of the risk of banking activities;
3. The absence or failure of key control structures and activities, such as segregation of duties, approvals, verifications, reconcilliations, and review of operating performance;
4. Inadequate communication of information between levels of management within the bank, especially in the upward communication of the problems;
5. Inadequate or ineffective audit programmes and monitoring activities.

Basel II discusses thoroughly the framework for internal control systems in banking organisations. It emphasises the fact that the bank's internal control structure is essential to the capital assessment process and indicates that effective control of the capital assessment process includes an independent review and, where appropriate, the involvement of internal or external audits. It goes on to point out that the bank's Board has the responsibility to ensure that management establishes a system for assessing the various risks, develops a system to relate risk to the bank's capital level, and establishes a method for monitoring compliance with internal policies. Further, the Board should regularly verify whether its system of internal controls is adequate to ensure well-ordered and prudent conduct of business (Basel II). An implication, as pointed out by Basel II, is that the periodic review of the internal control system is essential in order to ensure its integrity, accuracy, and reasonableness. Areas that should be reviewed include (Basel II, p. 167):

- Appropriateness of the bank's capital assessment process given the nature, scope and complexity of its activities;
- Identification of large exposures and risk concentrations;
- Accuracy and completeness of data inputs into the bank's assessment process;
- Reasonableness and validity of scenarios used in the risk assessment process;
- Stress testing and analysis of assumptions and inputs.

According to Basel II, the internal control framework consists of five interrelated elements (Basel II, p. 163):

- Management oversight and the control culture;
- Risk recognition and assessment;

- Control activities and segregation of duties;
- Information and communication; and
- Monitoring activities and correcting deficiencies.

This framework provides a response to risk breakdowns and identifies the principles, which should be followed for assessing the robustness of the internal control system including a specific requirement to recognise and address all risks facing the bank (Basel II).

The press has been frequently firing at the banking internal control deficiencies. Agence France-Presse (2008) reviews a particular area of interest in the internal controls related to Société Generale failure case caused by the misuse of the IT system in the bank and urges banks to be very cautious about the IT competitive advantage at the expense of the internal control standards. Palfi (2007) sees three main issues that banks need to address when looking at internal control. The first relates to capital adequacy and internal controls, which are in many ways a front line defence for shareholder's equity and depositor's funds. The second is the behavioural dimension of controls, which have increased tension in them in areas such as derivative trading where the line between trading and gambling is a narrow one. The third issue is whether the present overall system impairs operational efficiency due to the onerous and costly body of compliance requirements that have been established in a bank. Palfi (2007) argues that the latter point is particularly interesting because it highlights the potential for too much control in relation to the possible risk involved.

From a cultural perspective, internal control within the UAE commercial banking has been addressed by the CBUAE (2009), emphasising the need to understand the cultural differences within the UAE banking industry, and urging UAE banks to invest in developing innovative risk management methodologies, procedures and controls.

2.3.4.4.3 Operational Risk and Internal Control

Basel II places a bank's internal control system firmly at the centre of ORM. The term 'internal control' was incorporated on twenty five occasions in Basel II; which the author would contend could be interpreted as an indication of the importance of banking internal control systems in ORM.

Basel II proposes a framework consisting of fourteen principles that banking supervisors should use when evaluating a bank's internal control system, with paragraphs 20 to 23 examining risk assessment in the context of internal control systems. A risk assessment should regularly be carried out to evaluate the internal and external factors that could adversely affect the achievement of the banking organisation's operational, information and compliance objectives (Basel II). These are the main objectives of the internal control processes that should be in place, according to Basel II. The author would argue that the linkage of processes, operational risks and controls discussed previously in section 2.3.4.1, forms the basis by which Senior Management should ensure that the operational risks affecting the achievement of the bank's strategies and objectives are continually being evaluated.

Article 744 in Basel II provides guidance on how to maintain a sound internal control system: the bank's internal control structure is essential to the capital assessment process. Effective control of the capital assessment process includes an independent review and, where appropriate, the involvement of internal or external audits (Basel II). The article goes on to demonstrate that the bank's Board has the responsibility to ensure that management establishes a system for assessing the various operational risks, develops a system to relate operational risk to the bank's capital level, and establishes a method for monitoring compliance with internal policies. The Board should regularly verify whether its system of internal controls is adequate to ensure well-ordered and prudent conduct of business (Basel II). In short, Basel II emphasises the necessity for continuous monitoring, continuous review, capital adequacy verification, involvement of internal and external audits, and assuming clear responsibilities by the Board; in order to realise a sound internal control system. The author is of the view that this bouquet of activities should be affected in unison in order to achieve the desired objective.

Spira and Page (2003) analyse why sound internal control systems are fundamental to ORM. They review a number of well-known operational risk incidents involving fraudulent conduct and reckless management and find that the general consensus as to why they occurred is due to the critical absence of or failure to enforce proper internal control systems, internal audit of the control systems, and corrective actions to prevent opportunities for fraud, reckless management, or conflicts of interest.

Andreas (2010) points out that the greater emphasis on management and internal control requires bank supervisors to explore enhanced measures that strike a balance between prescriptive and principle-based control guidelines, which better reflects the economic reality of operational risk in light of the market failures during the Financial Crisis

The above discussion demonstrates that the implementation and monitoring of a comprehensive system of internal control within a defined framework is the key to ensuring that risk in general, and operational risk in particular, can be managed down to acceptable levels. An ongoing evaluation of internal control is, therefore, an important element in identifying operational risk exposures.

2.3.4.5 Corporate Governance

Corporate governance in the banking industry has become more prevalent over the last few years (Ciancanelli and Reyes 2001). BCBS published its initial guidance on corporate governance in 1999 (Basel 1999), with revised principles in 2006 (BCBS 2006) and 2010 (BCBS 2010). The guidance is intended to help ensure the adoption and implementation of sound corporate governance practices by banking organisations worldwide, but is not intended to establish a new regulatory framework. The guidance highlights the importance of the following (BCBS 2006, p. 47):

- The roles of the Boards, with a focus on the role of independent directors[32] and Senior Management;

[32] An independent director is member of the Board of directors of a company who does not form part of the executive management team. He or she is not an employee of the company or affiliated with it in any other

- Effective management of conflicts of interest;
- The roles of internal and external auditors, as well as internal control functions;
- Governing in a transparent manner, especially where a bank operates in jurisdictions, or through structures, that may impede transparency;
- The role of supervisors in promoting and assessing sound corporate governance practices.

Subsequent to the publication of the BCBS (2006) guidance, there have been a number of corporate governance failures and lapses, many of which came to light during the Financial Crisis. Drawing on the lessons learned during the Financial Crisis, BCBS published *Principles for Enhancing Corporate Governance,* 2010, which sets out sound practices for banking organisations in this regard. The key areas where the principles have been strengthened include: (1) the role of the Board; (2) the importance of an independent risk management function, including a chief risk officer (CRO) or equivalent; (3) the importance of monitoring risks on an ongoing firm-wide and individual entity basis; and (4) the Board and Senior Management's understanding of the bank's operational structure and operational risks BCBS (2010, p. 2 - 31). The principles also emphasise the importance of supervisors regularly evaluating the bank's corporate governance policies and practices as well as its implementation of the BCBS principles (BCBS 2010).

As pointed out by some of the interviewees in this research, the CBUAE is continually urging the UAE commercial banks to adopt the guidance set by BCBS (2010). The author

way. They are differentiated from inside directors, who are members of the Board who also serve or previously served as executive managers of the company (Higgs 2003).

considers this as a good move in the right direction. On the other hand, the author would contend that Boards which operate with heavy emphasis on monitoring management corporate governance practices may end up with less efficient performance. The implication of this proposition, if it were to be true, would suggest that the balance between operational risk and the level of management control needed is a fine one.

2.3.4.6 Operational Risk Mitigation

Deventer and Donald (2004) capture the essence of operational risk mitigation by maintaining that the challenge of ORM is to minimise the probability and magnitude of adverse events without incurring excessive cost.

Basel II discusses a number of techniques used to mitigate operational risk. The most important two mentioned are internal controls (which act to reduce the impact/probability) and insurance. This issue is taken up by Tsanakas and Desli (2007) who review the ways in which insurance can be used to mitigate operational risk.

Risk in banking is also mitigated when key decision-makers in organisations see the big picture Scandizo (2005). He goes on to point out that the organisation should be designed so that information about risk is communicated to those decision-makers who can put together warning signals from various areas in the organisation, thus forming a picture of a risky or hazardous situation in its early stages of development. The warning signals or KRI's are discussed in a banking context by Coleman (2007), who provides a number of examples of the indicators that may be used. He discusses, for example, data security risks

being controlled by backup files, password control, finger-printing and voice recognition. Computer viruses can be controlled by firewalls, monitoring computer usage, scanning software, stringent audit procedures and employee education.

According to Grody et al. (2007, p 44), selecting one or a combination of the following strategies is essential to the risk mitigation process:

- Avoiding the risk by suggesting alternative course of action;
- Eliminating the cause of the risk;
- Reducing the likelihood of the risk occurring;
- Reducing the direct consequences of the risk;
- Minimising the risk impact in business terms;
- Instigating further investigation to gather further information before a final decision is made;
- Accepting the risk as unavoidable.
- Transferring the risk.

The author would argue that whilst these are generic risk mitigation strategies, they can equally be applied to operational risk exposures.

2.3.4.7 The Measurement and Quantification of Operational Risk

Market risk exposures are typically quantified in terms of 'Value at Risk' (VaR) estimate (Dorfman 1997). The history of VaR is traced by Reed (1997) to Dennis Weatherstone, the Chairman of JP Morgan bank, who asked for a one page report to be delivered to him

summarising the company's exposure to moves in the market and estimating the potential losses over the next twenty four hours. Titus and Lewis (1997, p. 9) provide a definition of VaR, thus:

> "Value at Risk is the largest loss from market risk (expressed in currency units) that an asset or portfolio will suffer over a time interval and with a degree of certainty selected by the decision-maker."

VaR essentially defines the maximum a firm could lose given a certain level of confidence over a given time horizon, should exchange rates, interest rates and commodity prices move against it (Kevin 2005). The calculation of VaR in this context is well covered by a number of authors (see for example Titus and Lewis 1997, Kevin 2005, Vanita and Aggarwal 2008 and Abad-Romero 2009), and can involve a number of methods normally based on historical, empirical, simulated information or a combination.

The application of VaR approach in the area of operational risk (OpVaR) is, however; less developed, and Basel II guidelines offer three alternative approaches to 'valuing' operational risk with related qualifying criteria (Basel II, p. 140-150):

1. Basic Indicator Approach (BIA): calculates a value for operational risk capital using a single indicator as proxy for an institution's overall operational risk exposure;
2. The Standardised Approach (TSA): calculates a value for operational risk capital based on standard business units using a broad financial indicator (e.g. income) multiplied by a beta factor (i.e. proxy for the operational loss experience);
3. Advanced Measurement Approach (AMA): uses the bank's own internal current and historical loss data as well as external loss data, and a combination of qualitative and quantitative methods to calculate a value for operational risk capital.

The literature has a number of articles which deal with operational risk valuation (see for example Abernethy et al. 2004, Andreas 2007 and Dutta and David 2010).

Basel II postulates that banks still have work to do in adequately measuring operational risk exposures and need to move on a continuum from the BIA to the AMA, emphasising certain requirements for banks to qualify for using either of the TSA or AMA approaches (Basel II, p. 144):

- The bank Board and Senior Management, as appropriate, are actively involved in the oversight of the ORM framework;
- The bank has an ORM system that is conceptually sound and is implemented with integrity;
- The Bank has sufficient resources for the use of the approach in the major business lines as well as the control and audit areas.

According to Basel II, the AMA is meant to enable the bank to reduce the capital adequacy requirement since it is more sensitive to risk and more advanced and sophisticated than the other two approaches. Accordingly, Basel II imposes further requirement in order to ensure proper utilisation of this approach (Basel II p.144-150):

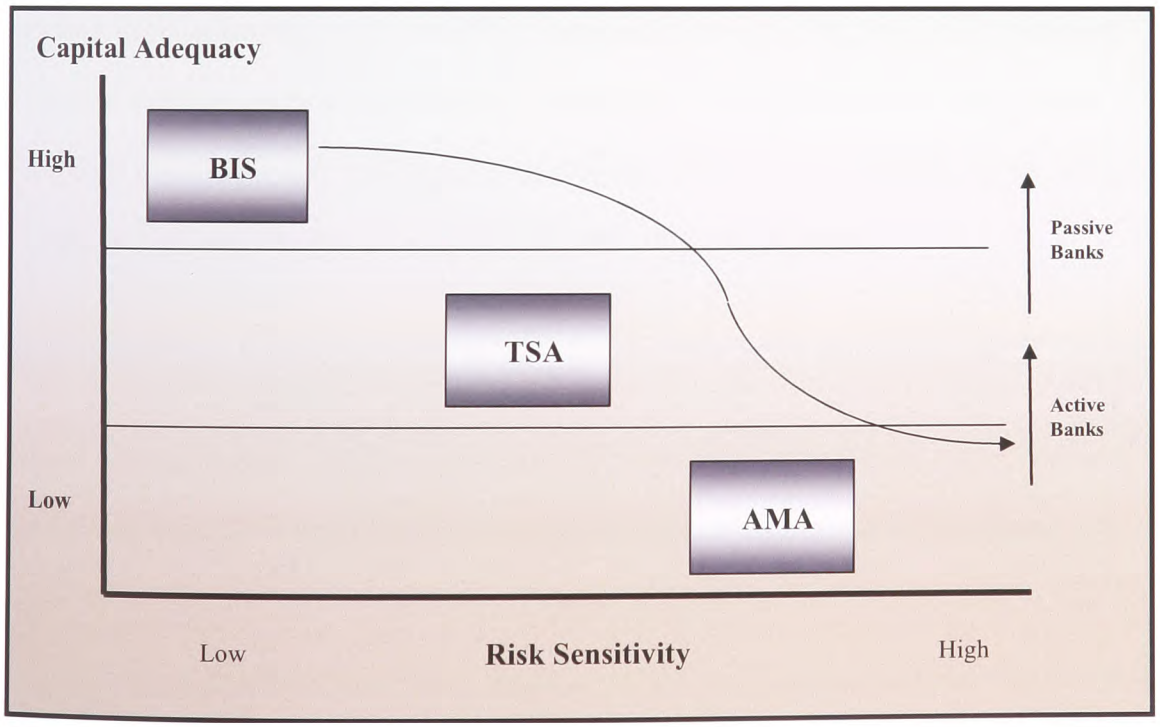
- The banks must track internal loss data based on a minimum of five-year observation period;
- The bank's operational risk measurement system must use relevant external data (either public data and/or pooled industry data), especially when there is reason to

believe that the bank is exposed to infrequent, yet potentially severe, losses. The external data should include data on actual loss amounts, information on the scale of business operations where the event occurred, information on the causes and circumstances of the loss events;

- The bank must use scenario analysis of expert opinion in conjunction with external data to evaluate its exposure to high-severity events. This approach draws on the knowledge of experienced business managers and risk management experts to derive reasoned assessments of possible severe losses.

Figure 9 illustrates the risk sensitivity versus the capital adequacy requirement for the three Basel II approaches.

Figure 9: Risk Sensitivity vs. Capital Requirement in Basel II



Source: Chaudhury (2009)

Chaudhury (2009) argues that the application of the BIA approach to measuring operational risk would be sufficient for most organisations to start with, however; banks need to look forward to the application of the AMA in order to reduce the capital adequacy requirement and to better safeguard themselves against operational risks (increase the bank's sensitivity to operational risk). According to a Manager interviewed in one of the banks:

> "The UAE commercial banks usually set aside capital for the unexpected and not the extreme since some operational risks may be easily quantified, while others are clearly impossible to quantify. Still, we make sure that we are in line with Basel II stipulations."

Another phenomenon of ORM and measurement is that various leading IT firms have embarked on research and analysis of the global market to produce risk management and measurement technology, with special emphasis on operational risk. The goal is to support financial institutes, as they drive business performance, through better risk management, corporate governance and compliance by providing in-depth analysis and actionable advice on the main aspects of operational risk (Gorrod 2004 and ACM 2005).

This brief analysis of operational risk measurement and quantification illustrates that there is still some work to do. Whilst operational risk measurement will remain an important goal in the long term, ORM will continue to remain the focus of attention for bank management.

2.3.4.8 Operational Risk Management Roles

A survey conducted by the researcher reveals that Basel II incorporates the bank's Board and Senior Management on thirty nine different occasions with emphasis on the important roles they carry out in ORM.

Basel II pins tremendous responsibilities on the Bank's Board and Senior Management for ORM. According to Basel II, the Board and Senior Management should ensure the development of a framework for assessing the various operational risks, a system to relate operational risk to the bank's capital level, and a method for monitoring compliance with internal policies. It is likewise important that the Board adopts and supports strong internal controls and written policies and procedures (Basel II).

Considering the above, Hubbard and Douglas (2009) emphasise that the key to ORM is management, a point taken up by Pagach and Richard (2010) who say that such management, if it is to act in the best interest of the owners of the business, should have character[33]. According to Aabo and Fraser (2007), effective risk management is the result of a sound risk management strategy that is grounded in the realities and the organisational culture, and has top management support.

A brief overview of the management structure required to manage operational risk in a trading environment is presented by Coleman (2007) who notes how financial institutions

[33] A person of character does what is right not because of a set of rules, or a reward structure, or because his/her actions will be noted by superiors, but because of the intrinsic merit or worth of these actions (Sheedy, 1999).

have been creating specialist Operational Risk Manager roles at a senior level. Their role is described as the creation of a group-wide culture of operational risk awareness. Coleman (2007) also points out that many institutions make use of their Internal Audit function to monitor the implementation of group risk policies, while deliberately excluding them from the actual formulation of rules about risk (a point which enhances their independence). Following the requirements of Basel II, the CBUAE (2008) has advised the UAE commercial banks to use either of the following organisational models for ORM:

- Head office driven: a centralised function that assumes the entire ORM responsibility, often supported by local Operational Risk Managers;
- Non-head Office driven: dedicated decentralised ORM units are in place in the business units.

The choice, whether to adopt the centralised or decentralised model, is left to the individual bank to decide based on the organisational requirements of the bank (CBUAE 2008). The data analysis results indicate that the UAE banks in this study opted for the second model.

2.3.5 Summary

This section has provided an analysis of risk management with a particular focus on operational risk. The concept of risk was discussed with the distinction between proactive and reactive risk management being noted. Risk pervades all aspects of society and business, and there have been a number of developments over recent years to produce a generic risk management model which can be applied to operational risk. However, the process is subjective and relies on people making judgements. Risk perceptions of

managers and individuals are, therefore, important in formulating these judgements. Risk perceptions were found to be linked closely to risk communication and the use of common risk language. Relevant theories were presented illustrating the complex nature of the subject.

The decision-making that takes place in the risk management process can be enhanced if the right information is made available to the manager. This was seen to be an important factor because there can be so many variables at play in making a risk management decision.

The literature review then focused on operational risk. It was noted that there had been a move towards more explicit (as opposed to implicit) ORM. There is a universally accepted definition of operational risk although there are a number of common themes around the definition that were reviewed and, generally speaking, the focus of operational risk is in the internal control environment. Operational risks were seen to be embedded in the processes (of the internal control systems), and were mitigated by the controls that management put in place. The reasons why operational risk has become important in the banking industry were identified and the scarcity of academic research about the UAE commercial banking was noted.

A distinction between ORM and operational risk measurement was noted, with the former being concerned with creating an adequately controlled internal environment and the latter being concerned with quantifying the total operational risk exposure. The two activities

appear to be mutually exclusive but both are recognised by the regulators as being highly important. A discussion on the Value at Risk (particularly in the market risk area) concept was presented, although it was noted that there was still some way to go in the operational risk measurement area. Fraud, the regulatory environment and corporate governance, three areas of interest to ORM, were examined. The section concluded with a review of the ORM roles.

2.4 Banking

2.4.1 The UAE Commercial Banking Industry Structure

The literature review found little literature on the UAE commercial banking environment. Hence, this section will discuss the commercial banking in general, and focus on the UAE commercial banking as much as possible.

The number of different players in the UAE financial industry as on Dec. 31, 2010 is depicted in Table 3[34] below.

[34] Table 3 represents the list of banks and other financial institutions licensed by the CBUAE to conduct banking financial, investment brokerage and money-changing activities as on Dec. 31, 2010 (CBUAE 2010).

Table 3: List of Banks and Other Financial Institutions in the UAE

S. No.	Description	Head Offices	Branches
1.	**Banks**		
	A: National Banks – non Islamic B: National Banks – Islamic C: Foreign Banks	18 6 28	693 102 153
	Total	**52**	**948**
2.	Investment Bank	2	-
3.	Wholesale banking (high value transactions)	2	-
4.	Finance Company	24	24
5.	Representative Office	98	
6.	Investment Company	20	
7.	Banking Consultant Financial and Investment Company/Est.	13	1
8.	**Money and Financial Brokers**		
	D: Currencies and Commodities Brokers E: All Financial Brokers	6 6	1 1
	Total	**12**	**2**
9.	**Moneychanger Company/Est.**		
	F: Sell and Buy Currencies and Cheques G: All money-changer activities including Transfers	12 99	6 499
	Total	**111**	**505**
	Total for all licenses	**334**	**1480**

Source: Adapted from CBUAE (2010)

Table 3 indicates that there are a total of forty six commercial non-Islamic banks in the UAE. This number has substantially increased over the last few years as a result of the excessive liquidity of such an oil-rich tax-free country (Saif and Choucair 2009).

During the last few years, the UAE commercial banking industry has been witnessing structural changes resulting from:

- The GCC single currency programme that has set in motion a rationalisation process which would have a dampening effect on commercial banking traditional approach to business (Al-Suwaidi 2010).

- The Financial Crisis: Saif and Choucair (2009) argue that as a consequence of the Financial Crisis, the banking sectors in the UAE generally suffered despite the continued improvements and strengthening of banking supervision. They go on to point out that the UAE economy and its banking sector got the ultimate confidence boost as it received assurance from the UAE Government which approved a set of preventive steps and measures to serve the national interest and protect the national economy (Saif and Choucair 2009, p. 9):

    - ✓ Pumping United Arab Emirate Dirham (AED) 120 billion into the banking sector to deplete fears of a financial meltdown;
    - ✓ Guaranteeing depositors' money in national banks;
    - ✓ Guaranteeing inter-bank lending between national banks.

The author would contend that the measures set by the UAE Government reduced the impact of the Financial Crisis on the UAE commercial banks by providing liquidity to banks and comfort to depositors:

- Dubai Crisis: As a result of the worldwide economic downturn following the Financial Crisis, Dubai suffered a major economical deterioration (Simon 2009). Many property construction projects came to a sudden halt resulting from the sudden decline in demand due to negative economic expectations (Hazelton 2009). Hazelton (2009), points out that depositors became uncomfortable with keeping their savings in banks due to the contagion effect of the USA bank failures. As a result, the UAE banks suffered from lack of liquidity; which added salt to injury.

The UAE Government intervened in a timely manner to restore confidence in the UAE commercial banks as indicated above.

- Stock Exchange crisis: During 2004 - 2006, there were significant increases in the volume of shares traded and the share prices of many companies. However, towards the end of 2006 and through the first few months of 2007 the bubble burst and share values dropped by more than 70% (Huberman 2007), along with similar and parallel decreases in UAE. As a direct result, credit defaulting in commercial banks became a common trend with the consequence of reducing liquidity and profitability (Gulfnews 2007).
- UAE currency pegging change rumors: Since the year 2005, there were frequent rumors that, due to the declining US$ rate, the UAE was planning to change its currency pegging from the US$ to another currency IMF (2005). As a consequence, many worldwide depositors used the UAE commercial banks as a potential means for profit generation had the pegging change been affected, expecting the UAE currency would appreciate. CBUAE (2009) declared in a press conference that there would be no currency pegging change. Driven by the Financial Crises, the majority of foreign depositors withdrew their cash in droves, leaving the UAE commercial banks to suffer from lack of liquidity (Gulfnews 2009).

Bearing these factors in mind, a report by the Business Review Weekly (2008) identifies four additional forces that are driving the UAE commercial banking industry[35] to change the way it operates:

[35] This study was undertaken in the Emirates of Dubai and Abu Dhabi.

1. Consumer demand: consumers are demanding fast, convenient, glitch-free service from the branches and non-premise distribution channels;
2. Technology development: many UAE commercial banks have built sophisticated information management capabilities that will help them to enhance their consumer management capabilities;
3. Competition: new customer acquisition strategies are intensifying whilst revenue generation is growing more complex, more difficult and costly;
4. eCommerce[36] (Internet banking or on-line banking) and mBanking[37, 38] (mobile banking): eCommerce and mBanking are set to dominate the way business to customer (B2C) and business to business (B2B) transactions are undertaken.

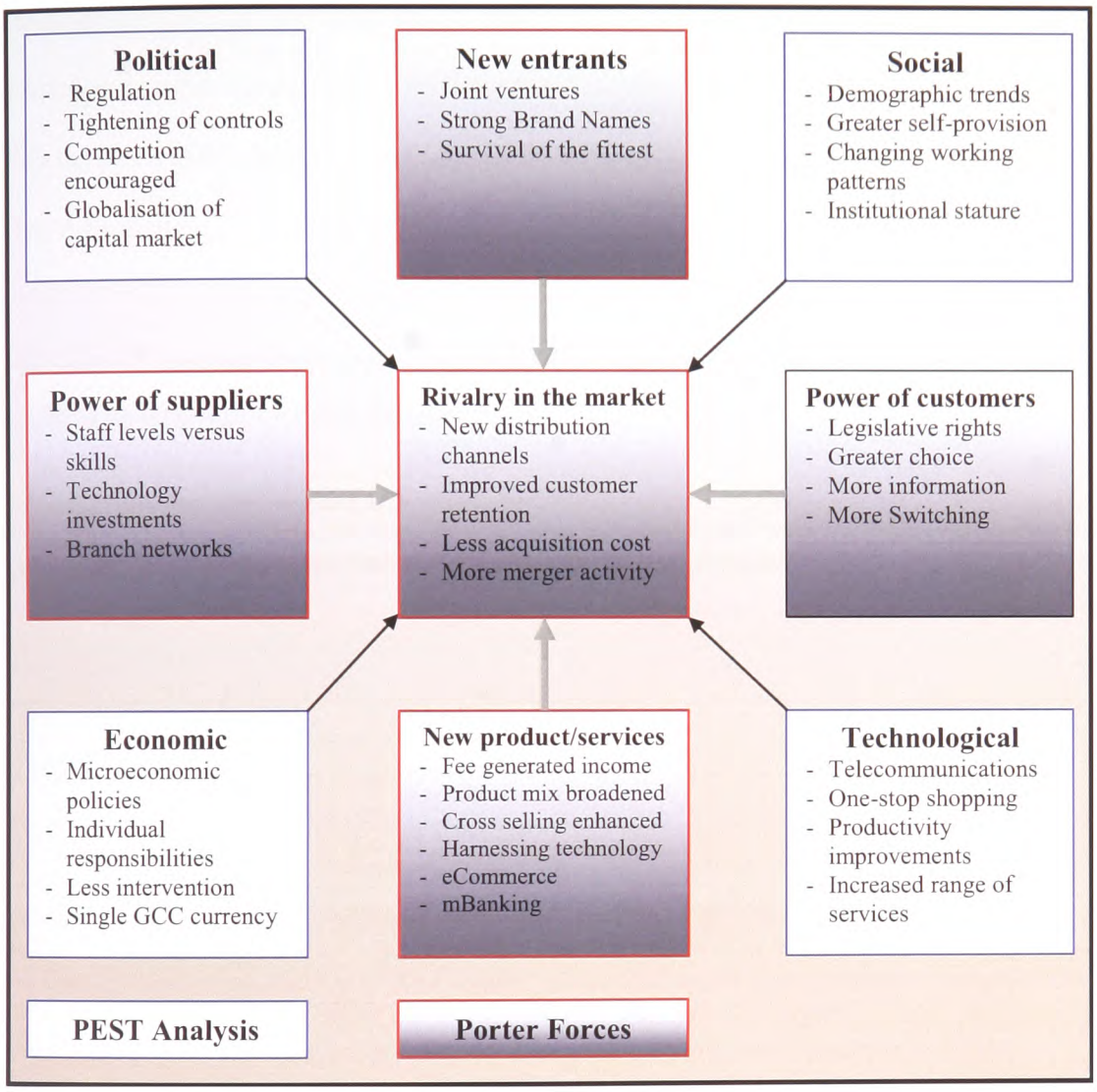
Underlying these forces, Gulfnews (2008) looks at the drivers behind the change in the UAE commercial banking industry at the macro level, i.e. development in the wider business environment commonly known as a PEST (political, economic, social and technological) analysis, and the micro level, i.e. based on the five forces model of Porter (1985). The analysis is represented diagrammatically in Figure 10.

[36] eCommerce (also known as Internet banking or on-line banking) consists of the buying and selling of products or services over electronic systems such as the internet and other computer networks (Graham 2008).

[37] mBanking (also known as Mobile banking) is a term used for performing balance checks, account transactions, payments etc. via a mobile device such as a mobile phone (Tiwari and Herstatt 2007).

[38] The author of this thesis is heavily involved in mobile banking and financial services network deployment via mobile telephony networks in many countries in the world (to name a few: UAE, Cote D'Ivoire, Benin, Gabon, Togo, Niger, Nigeria).

Figure 10: Forces Driving Change in the UAE Commercial Banking



Source: Adapted from Gulfnews (2008)

There are examples to support the development of these forces and some writers have illustrated some of the themes in the diagram. For example, Mustapha (2008) looking at the most efficient methods for regulating the UAE banks (political analysis) argues for even greater regulation by CBUAE because bank regulation, especially capital requirements,

induces bank stability. Mansur (2008) suggests that the UAE banks, in facing these challenges should not lose site of one of their most valuable intangible assets, namely, their institutional stature (social analysis). He argues that whilst customers are not quite happy with the services that banks deliver, they still trust their banks as a safe and secure place to keep their money.

2.4.2 The Regulatory Environment

2.4.2.1 Banking Regulation Historical Review

The history of banking regulation in the UAE can be traced back to 1980 when it became possible for banks to shed their constitutions and acquire the benefits of incorporation as either limited or unlimited companies CBUAE (1980). According to the World Fact Book (2010), the CBUAE took several measures in the early 1980's to strengthen the banking structure. It expanded audits and inspections, increased bank reporting requirements, established a computerised loan risk department, and set minimum capital requirements. On Dec. 2, 2008, the CBUAE (2008) issued its mandate to the UAE commercial banks via Notice 4170/2008 that they ensure that they fully adhere to Basel II operational risk recommendations by Jan. 1, 2011. With this mandate, the author argues, the 'disconnect' in the UAE commercial bank regulation has been addressed.

Worldwide, the degree of governmental monitoring became more crucial to improving the stability of the banking sector, and continuing bank failures in the 1920's and 1930's are generally accepted as the cause for further extensive bank regulations being introduced across many countries (Hickson and Turner 1996). By that time, minimum capital

requirements were being imposed on banks (Hickson and Turner 1996). The momentum continued around the globe with a range of different regulatory requirements being used. Nevertheless, banks continued to have problems and it was not until the 1980's, when concern about international banks financial health mounted and complaints of unfair competition increased, that the BCBS started considering proposals to set capital standards for the banks (Freixas and Santomero 2003). In 1988, when Basel Accord I came into being, it was seen as a breakthrough in regulation. For the first time, regulators from a number of countries had set a truly global standard for capital adequacy in relation to banking operations.

Basel I explicitly covered credit risk. It required banks from the G10 countries to hold a minimum capital adequacy equal to 8% of risk-adjusted[39] assets. In 1996 an amendment to the accord introduced market risk exposures and, as noted by Santos (2000), the main novelty of the amendment was that it allowed banks to use their own internal models to determine the required capital charge for market risk. VaR, the Value-at-Risk (see section 2.3.4.7) concept had now entered into the regulatory regime.

The reader will note the focus on the risk that the Basel I introduced was geared towards credit risk followed by market risk. Operational risk was not specifically mentioned but interest in this area probably grew as a result of the banking collapses, which derived from operational risk failures (e.g. Barings). Accordingly, Basel I had a serious drawback in that

[39] The calculation of risk adjusted assets involves taking both on- and off-balance sheet items and assigning them to risk category which would weigh them (by factors of 0%, 10%, 20%, 50% and 100%) according to the perceived riskiness of the assets (Basel I).

it adopted a 'one size fits all' approach and did not address operational risk (Santos 2000). To address these issues, BCBS published its second accord (Basel II) which is meant to take into account the shortcomings of the previous one. According to Moosa (2007a), Basel II was designed to be more flexible and risk sensitive as highlighted in Table 4.

Table 4: High Level Comparison between Basel I and Basel II

Basel Accord I	Basel Accord II
Addressed credit rand market risks.	Addressed credit risk, market risk and placed special emphasis on operational risk.
Focused on a single measure.	More emphasis on banks own internal methodologies, supervisory review, and market discipline.
One size fits all.	Flexibility, menu of approaches, incentives for better risk management.
Broad brush structure.	More risk sensitive.

Source: Adapted from Moosa (2007a)

The structure of Basel II is based on three mutually reinforcing pillars. Together these are seen as contributing to the safety and soundness in the financial system. The pillars cover (Basel II, p. 182 – 184):

- Pillar 1: minimum capital requirement - this is still set at 8% of risk-weighted assets; a measure for operational risk is included whilst market risk remains unchanged.
- Pillar 2: supervisory review process – requires supervisors to ensure that each bank has sound internal processes in place to assess the adequacy of its capital based on a thorough evaluation of its risks.

- Pillar 3: market discipline – aims to bolster market discipline through enhanced disclosure by banks including the way a bank calculates its capital adequacy and its risk assessment methods.

Aabo and Fraser (2007) note that the scene has, therefore been set for banks to focus their risk management and measurement techniques in the early years of the 21st century and for the first time operational risk features directly in the assessment of capital adequacy. Basel II points out that whilst measuring capital is one thing, it is important not to lose sight of the function of capital itself. Capital is only one important tool in the overall supervisory arsenal. Supervisors are likely to be playing a more active role in monitoring a bank's capital adequacy and risk management arrangements (Basel II).

As discussed in section 1.1.1, BCBS published its third Capital Accord in December 2010: "*International Framework for Liquidity Risk Measurement, Standards and Monitoring*" in response to the deficiencies in the financial regulation revealed by the Global Financial Crisis from liquidity risk perspective, hereafter; referred to as Basel III. Nevertheless, in this study, there will be more focus on Basel II for two reasons:

1. Basel II is more concerned with operational risk management, measurement, sources and other operational risk areas (Basel II, p. 140 - 152); whereas, Basel III is concerned mainly with liquidity risk management (Basel III, p. 1).
2. Basel III is not due for final implementation, yet. It will officially be introduced in two stages: January 2015 and January 2018. Until then, Basel III will undergo analysis of financial institution feedback, monitoring and updating (Basel III, p. 41)

The author considers the enforcement of Basel III and the consequent implications for ORM an interesting area for further future research.

The discussion in this section reveals that the regulations and competitive pressures on the UAE commercial banks are, therefore, set to increase on a number of fronts. This provides further impetus and support for this research project with its emphasis on understanding how the UAE commercial banks are mitigating the operational risks that confront them.

2.4.2.2 Bank Stress Testing

Nelson (2004) explains stress testing as a form of testing that is used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results. In the case of banks, testing is conducted under assumptions of deteriorating economic conditions, such as low gross domestic product (GDP)[40], higher unemployment rate and lower real estate prices. The purpose of the test is to ensure that banks have enough capital to survive (Nelson 2004).

BCBS (2008) emphasises the importance of stress testing. It advocates that it is important to note that stress testing is especially favourable after long periods of good economic and financial conditions, when fading memory of negative conditions can lead to the under evaluation and estimation of risk. It is also a key risk management tool during periods of

[40] Gross domestic product (GDP) refers to the market value of all final goods and services produced within a country in a given period. It is often considered an indicator of a country's standard of living (Lequiller et al. 2006).

expansion, when innovation leads to new products that grow rapidly and for which limited or no loss data is available (BCBS 2008). Jokivuolle et al. (2008) conclude that BCBS (2008) requires banks to conduct stress tests on their potential future minimum capital requirements and consider the effect of the Financial Crisis scenarios.

BCBS published its *"Principles for sound stress testing practices and supervision"* BCBS (2009). The committee points out that stress testing is an important risk management tool that is used by banks as part of their internal risk management, and is promoted by regulators through Basel II. BCBS (2009) further points out that stress testing alerts bank managements to adverse unexpected outcomes related to a variety of risks and provides an indication of how much capital might be needed to absorb losses should large shocks occur.

Chopra (2009) argues that drawing on the lessons for banks and supervisors emerging from the Financial Crisis, BCBS (2009) work presents sound principles for the governance, design and implementation of stress testing programme at banks. It addresses weaknesses in stress testing exposed by the Financial Crisis, including the specific areas of risk mitigation (Chopra 2009).

According to BCBS (2009, p. 1), stress testing is a tool that supplements other risk management approaches and measures, and plays a particularly important role in:

- Providing forward-looking assessments of risk;
- Overcoming limitations of models and historical data;
- Supporting internal and external communication;

- Informing the setting of a banks' risk tolerance;
- Facilitating the development of risk mitigation or contingency plans across a range of stressed conditions.

The author shares the view of Chopra (2009) that this is an interesting bouquet of benefits that banks can accrue from conducting stress testing to help shield themselves against operational risks.

Recently, two bank stress testing exercises were conducted:

1. The Supervisory Capital Assessment Programme (SCAP) was an assessment of capital conducted in February 2009 by the Federal Reserve System and Supervisors to determine if the largest USA financial organisations had sufficient capital buffers to withstand the recession and the financial market turmoil (SCAP 2009). The capital levels at nineteen institutions were tested. The test revealed that only nine banks had sufficient capital to withstand the recession and the financial market turmoil. Failed banks were given a grace period of six months to close the capital deficit gap (Wall Street Journal-WSJ 2009).
2. European Union-wide banking stress test exercise was conducted by the Committee of European Banking Supervisors (CEBS) in July 2010. The Council of the European Union mandated the CEBS to do so, in the aftermath of the global Financial Crisis (Organisation for Economic Co-operation and Development–OECD 2010). The exercise assesses the financial strength of European banks under different adverse scenarios. The exercise was conducted in cooperation with the

European Central Bank, the European Commission and the national supervisory authorities of the member states. The test revealed that eighty four banks had sufficient capital to withstand the recession and the financial market turmoil. Failed banks were given a grace period of six months to close the capital deficit gap (OECD 2010).

The results of these two test support the view of Chopra (2009) cited above. However, an issue faced by banks undergoing stress testing is whether the tests would decrease confidence in any bank that performs badly under the test (Chopra 2009). The author would argue that the latter point can be very critical to certain banks since it may reflect on the reputation of the bank.

The literature review reveals that no stress testing exercises were conducted on the UAE commercial banks; a fact which the author also argues may be due to the reputational issue mentioned above. Having said that, and given the importance of bank stress testing, it begs the questions: When will the CBUAE mandate the UAE commercial banks to conduct stress testing? Are the UAE commercial banks prepared for undergoing stress testing? The author considers this to be an area worthy of further research.

2.4.3 Information Technology and mBanking

The rapid advancements in technology have a major impact on the competitive structure of banking systems Annamalah (2008). Banks use IT extensively in carrying out their day-to-day operations, most notably in the areas of electronic cash dispenser networks and more

recently in the areas of telephony and internet banking systems, or the so called eCommerce (Arnaboldi and Claeys 2008). The development of the internet has removed one of the main barriers in commercial banking, i.e. the cost of setting up a branch network (Graham 2008). Internet only banks in the UAE such as 'Bank4me' attest to the extent to which information technology may be put in developing a banking operation.

IT is also becoming important in the generic area of risk management for banking operations. Aref (2009) in his review of information technology for risk management highlights that many financial institutes have risk management support systems already in place (the so called DSS) whereas many others have already started the deployment process. The interviews conducted in this research reveal that the majority of the UAE commercial banks are in the process of deployment of risk support systems; however, no literature was found in this regard. A number of worldwide information technology firms have developed software to support ORM, and an examination of operational risk journals (such as Journal of Operational Risk, Operational Risk and Regulation, OpRisk Compliance) reveals that these journals frequently carry advertisements for such products.

Another trend of advanced technology that is growing rapidly in the banking sector is the mobile financial services/mobile-banking, or so called, mBanking. This type of services necessitates the technical and operational partnership of the mobile network operator and a bank that has a large foot-print in a specific region (Tiwari and Herstatt 2007). The literature review reveals that mBanking has been well researched (see for example Tiwari

and Herstatt 2007, Cheney and Julia 2008), giving an indication of the importance of this thriving technology in commercial banking.

Cheney and Julia (2008) demonstrate that financial institutions are considering how and to what extent to incorporate mBanking into their business models. The evolutionary path taken by mBanking is substantial and depends on a variety of factors besides available technologies and experience with related products (Cheney and Julia 2008, p.13). Such factors include:

1. Consumer adoption of mobile cellular phones and associated non-voice communication technologies;
2. Consumer adoption of contactless payments;
3. Data security considerations.

Cheney and Julia (2008) argue that the emerging adoption patterns also raise risk, policy and business model considerations, data security considerations, and coordination issues. They go on to point out that ultimately, greater adoption will rest on the ability of market participants and regulators to work together in order to market and regulate products and services that combine a telecommunications device and a payment process into an innovative way to connect consumers with banks. With the anticipated success, the mobile channel may become the primary way through which consumers conduct their banking business, particularly in developing economies without comparable alternatives (Cheney and Julia 2008).

Vince (2008, p. 29) is more specific in reviewing a range of mobile banking products that are already in use in many countries:

1. mWallet (CashIn/CashOut): the mobile telephony network subscriber can deposit funds in a virtual wallet associated with his subscription to the mobile network, created by the mobile telephony network operator.
2. mBill Payment: the mobile telephony network subscriber can pay his bills and merchandise value using his mWallet.
3. Money Transfer via mWallet: the mobile telephony network subscriber can transfer funds to another mWallet belonging to another subscriber on the network. This is called Peer to Peer transfer (P2P), and has two forms: national and international transfer.

The author would contend that eCommerce and mBanking are becoming two major trends in banking evolution for years to come. The drawback is that with technology comes risk and in particular operational risk that needs to be addressed as early as possible. The literature review reveals that operational risk in mBanking has not been researched, and hence, can be an interesting area for future research.

2.4.4 Implications for Operational Risk Management

There are a number of implications for ORM emerging from the review of the issues facing commercial banks in general and specifically, in the UAE. The industry structure is changing and with change comes risk. Regulation, in particular, is a key driver behind changes at the macro and micro levels, and the UAE commercial banks will have to ensure

that they are ready to face the challenges being imposed by the regulatory regime, with its increased emphasis on ORM. The drivers of ORM are also coming from competition and new technologies. New entrants into the market already have their customer bases through which they can offer products. The UAE commercial banks will have to respond to these threats by taking more risks to secure their business and avoid customers leaving them in droves. New technologies, particularly eCommerce and mBanking, bring new opportunities as well as new risks and commercial banks will need to ensure that their developments in this area are managed with the potential risks in mind. The literature review reveals that operational risk has not been adequately addressed in eCommerce and particularly, in mBanking (Malphrus 2009).

Customers are becoming more demanding and the marketing mix is changing with a much broader range of products being offered and supported by banks. All these have implications for operational risk as the banks react and change the way they do business. One specific example which has been previously cited is the movement of commercial banks into the mBanking market. This has brought increased operational risk with new processes and internal control requirements, but, it may also increase the cooperation between banks and mobile network operators, and their understanding of each other's business.

2.4.5 Summary

This section provided an overview of the current challenges being faced by the UAE commercial banks and illustrated how these challenges will impact upon their operational

risk profile. A review of the macro level commercial banking industry structure was followed by an examination of several key areas, with a specific focus on the regulatory regime, which is one of the main drivers of this study. A discussion on risk management in the current banking environment confirms a number of complexities and issues that will need to be proficiently managed. The section concluded with a review of the implications for ORM.

2.5 Summary of the Literature Review

The UAE commercial banks are currently subject to much environmental uncertainty in the area of operational risk. This is being driven by a number of factors including the regulatory situation, the Financial Crisis, Dubai Crisis and the move for a GCC single currency.

Bearing this in mind, this Chapter has reviewed the literature in the areas of management and organisations, risk management; with specific emphasis on ORM, regulatory environment, and finally banking. The focus has been to describe relevant theories in the context of ORM and also to provide an overview of some of the current issues in each of the areas. The author has not attempted to describe each area in detail, as this would be beyond the scope of this research. A relevant thorough discussion is, however, warranted in order to place the research into an appropriate theoretical framework and illustrate to the reader the importance of the research in the context of the current business environment.

Section 2.2 provided some theoretical propositions relating to organisations, management within organisations, how the organisations cope with environmental factors and decision-making. It was noted how contingency theory can play a part in both the organisational structure and the decision-making process. The behavioural aspects of management and the internal environment in which they have to operate also feature in the day-to-day decisions that managers have to make. The theory of bounded rationality as it is described, identifies one of the barriers to decision making and is seen as important in the context of operational risk mitigation, which involves making a decision about the most appropriate action to take.

Risk management with particular focus on operational risk was discussed in section 2.3. The concept of risk was discussed with the distinction between proactive and reactive risk management being noted. Proactive risk management uses a generic risk management process model to manage risk whereas reactive risk management is, in effect resolving a problem that has occurred. The overall context in which risk management takes place is rooted in the contingency theory and underpinning this are a number of other theoretical propositions relating to risk perceptions, or how the managers who have to manage risk view the risk they have to manage. The risk perception can be enhanced if the right information is made available to the manger before the decision is made.

In the operational risk area, it was noted that there had been a move towards more explicit (as opposed to implicit) ORM. There is a universally accepted definition of operational risk and there is agreement that operational risks are mainly embedded in the bank's internal

control systems. A distinction was also made between ORM and operational risk measurement. This point is important when viewed in the regulatory context because whilst Basel II discuss the two activities, it is not clear whether they are viewed as mutually exclusive. To date little work appears to have been done on integrating the two.

Section 2.4 was focused on the current challenges being faced by the UAE commercial banks and illustrated how many of these challenges will impact upon their operational risk profile. The competitive climate in the UAE is intensifying and the range of products and services offered by banks, financial investment firms, money changers, real estate financing companies are almost identical. In this type of climate, differentiation and brand strength can add a lot of value to the customer proposition, and he or she in turn may then be influenced to buy the name first followed by the product.

Several key areas in the regulatory environment illustrate the importance and timeliness of this study. Basel II has introduced a major shift towards even more explicit ORM as well as forcing the pace of change on how operational risk should be measured. Banks have always been in the business of taking risks and the discussion on risk management confirms the need for banks to establish clear risk policies that were understood by all as a first step to preventing some of the disasters that have beset the banking industry over the last few years. Bank stress testing and the Basel III which is geared at improving liquidity risk management have also been discussed. Basel III will be introduced in two future stages: January 2015 and January 2018.

Following this review of some of the theoretical perspectives of ORM, the remainder of the thesis examines ORM (and mitigation) in practice. Chapters 3 describes the overall research design and the methodology that have been employed to collect and analyse the data. Chapter 4 provides analysis of the results of the data collected from the case studies; Chapter 5 considers the implications and conclusions of the findings for the groups arguably most interested in ORM: Risk Managers, the Operational Managers in the Business Units and Internal Auditors; and Chapter 6 provides a summary for the research and suggestions for further future research.

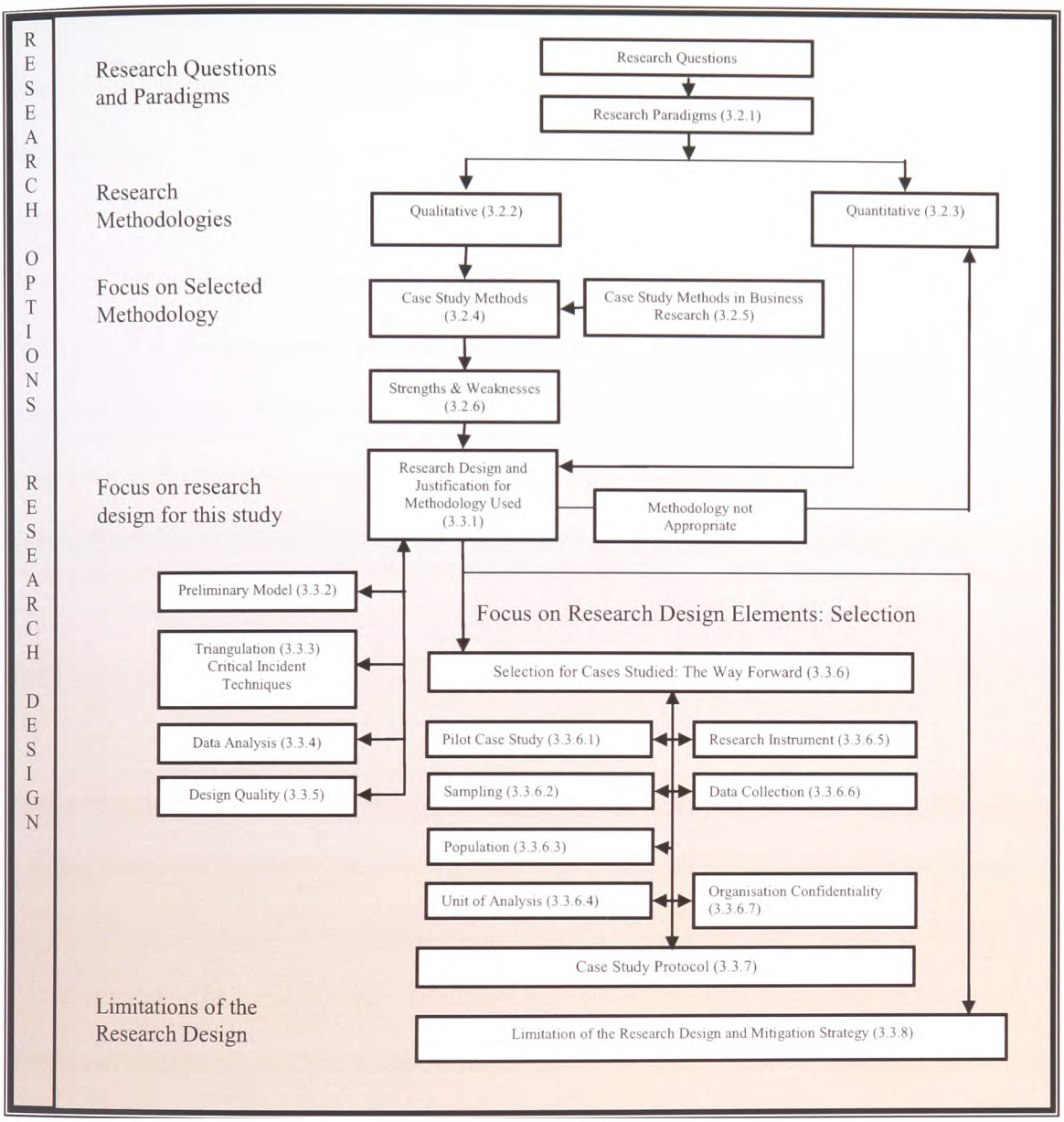
3. METHODOLOGY

A description of the research methodology and the logic for using the particular research approach is described in this Chapter. Following an overview of the proposed methodology (section 3.1), the structure of the main items of the remainder of this Chapter is shown in Figure 11. This Chapter is broadly divided into two main parts:

1. Research options: linking back to the research question, section 3.2 examines research paradigms, the two main research approaches and then focuses on case study methodologies as the most appropriate option for answering the research question;
2. Research design: section 3.3 focuses on the research design for the study and argues for the methodology used. It includes the following subsections:

   3.3.1 Research Design
   3.3.2 Preliminary research Model
   3.3.3 Triangulation
   3.3.4 Data Analysis
   3.3.5 Quality of the Research Design
   3.3.6 Selection for the Cases Studied: The Way Forward
   3.3.7 Case Study Protocol
   3.3.8 Limitations of the Research Design and Mitigation Strategy

Figure 11 Structure of Chapter (3) Showing Sectional Links



Source: Developed by the author

3.1 Methodology – In Outline

According to Patton (2002) all research strategies are seriously flawed, as the very strengths in regard to one desideratum function as weaknesses in regard to other equally important goals. He goes on to advise researchers that they should be aware of the dilemmas facing them and be fully armed with possibilities on how to handle them. Creswell (2003) describes the research process as a taboo, arguing that the traditional model of research is presented as an idealised model but when confronted with reality, researchers, and particularly student researchers, realise that the process is characterised by complexity and intractability (difficulty in manipulating). Such truisms reinforce the need for the researcher to describe objectively his research methodology, the methodological position adopted and the appropriateness of the methods used to the research questions posed.

The theoretical foundation upon which the research is based has been described in Chapter 2, where the research problem was placed in the wider body of knowledge. The research is described as largely exploratory because no prior work was found to have been undertaken in this area in the UAE and the research output may be viewed as building blocks for operational risk mitigation. The focus of the study was to collect data that would answer the research questions and enable a risk mitigation model to be developed. From the beginning the author was keen to model the practices in the field of operational risk mitigation in the UAE commercial banks.

The data was collected using multiple exploratory case studies. An initial pilot case study was undertaken to test the appropriateness of the key issues and revise the case study protocol which was based on that suggested by Straits and Singleton (2006). Four UAE commercial banks were selected and four or five managers within each of the banks were interviewed (see section 3.3.7.4). From the beginning it was hoped that the opportunity to discuss the day-to-day issues concerning ORM would provide a rich insight into the emerging practices. The author was equally concerned to ensure that the research deliverables would help managers in mitigating operational risk. Managers treat models as tools (George and Bennett 2005). Their primary goal is to use models, and the knowledge that they bring, to achieve organisational goals[41]. The scientific validity of this knowledge is of lesser importance to managers than its practical usefulness (George and Bennett 2005). The managers were the unit of analysis within the study and each case was treated as a separate entity before cross-case analysis and comparison was undertaken.

For reasons of confidentiality, the banks in question cannot be named and each has been referred to by a Greek letter; however, the bank names were made available to the research supervisor. The author was keen to study banks that were appropriate for the type of exploratory research envisaged. Gerring (2005, p. 37) notes the following in this context:

> "Work should take place in fast-moving companies operating in rapidly changing environments so as to provide illustrations of developing good practice at the leading edge of adaptive activity."

[41] The author is aware from some of the interviews that some of these goals are linked to the management of risk within the organisation.

The author is vigilant about using the term 'good practices' when discussing operational risk in the financial services sector of the UAE. Whilst operational risks have existed within the UAE commercial banks for many years, the literature review shows that explicit ORM has started only recently. A few years ago, the term operational risk did not even exist in the financial services in the UAE and the management of such risks was done implicitly as part of the day-to-day responsibilities. It is for this reason that the term 'good practices' has been used. Notwithstanding this position, all the selected banks operate in the rapidly changing UAE commercial banking sector and each has been subject to significant change, over the course of the last few years.

The epistemology (knowledge) behind the research is rooted in post-positivism[42]. Whilst post-positivism accepts that empirical observations are important, it rejects the idea that such observations are an immutable or absolute foundation for knowledge claims (Philips and Nicholas 2000 and Zammito 2004). This is not to say that a positivist[43] approach cannot be used within a case research methodology. The author has focused his work on providing a theoretical grounding, multiple sources of evidence (including the use of *Critical Incident Techniques*) and on persuasiveness of logical argument (Flyvbjerg 2006).

[42] Post-positivism is a meta-theoretical stance that critiques and amends positivism. Post-positivists believe that human knowledge is based not on unchallengeable, but rather upon human conjectures (propositions that are unproven but appear correct and have not been disproven). As human knowledge is thus unavoidably conjectural, the assertion of these conjectures is justified by a set of warrants, which can be modified or withdrawn in light of further investigation (Zammito 2004).

[43] Positivism refers to a set of epistemological perspectives of science which hold that the scientific method is the best approach to uncovering the processes by which events occur (Cohen and Maldonado 2007).

A research process was developed at the start of the study as a means of guiding the work. Data was collected using, primarily, semi-structured interviews, and from a variety of sources including press articles, annual reports, internet material and relevant internal documents (reports/ memoranda/manuals/presentations). Most interviews averaged three hours each and all interviews were taped and transcripts sent to the interviewees for correction. For each case study a detailed report was produced and sent to the lead contact in the bank for corroboration. A follow-up discussion about the findings was then arranged. The interviews were held during the year 2010.

To summarise, the research methodology involved developing a set of research questions and a preliminary model based on the literature review. The model was used to focus the work in the principal area of interest, that is, operational risk mitigation. Multiple exploratory case studies were used to collect data. Data triangulation was employed using *Critical Incident Techniques*. According to O'Donoghue and Punch (2003), triangulation is a method of cross-checking data from multiple sources to search for regularities and irregularities in the research data. Altrichter et al. (2008) contend that triangulation gives a more detailed and balanced picture of the situation. A pilot case study was used as a basis for refining the case study protocol and the research model itself was revised and updated in the light of the research findings.

3.2 Research Methods in Perspective

3.2.1 Research Paradigms

The author started this research recognising that positivist beliefs appear to have dominated the research in the physical and social sciences over the last fifty years but equally noticing the trend towards using post-positivist methodologies.

Researchers have an obligation to fully describe their theoretical posture[44] (Kincheloe 2005) in order that the critical reader can understand how he or she construes the shape of the social world in which he or she operates, particularly in the context of the research project itself.

To identify where the post-positivist paradigm fits in the qualitative research approach, it is necessary to examine the research process itself and then consider how the different paradigms fit within this process. Guba and Lincoln (2005, p. 93) summarise the qualitative research process into phases, which are reproduced in Table 5.

[44] Posture may be defined as the relationship that the researcher wants to have with the subject being researched (Pereira et al. 2003).

Table 5: The Research Process

Phase 1	**The Researcher as a Multicultural Subject** • History and research traditions. • Conceptions of self and the other. • Ethics and politics of research.
Phase 2	**Interpretive Paradigms** • Positivism, post-positivism. • Constructivism • Feminism. • Cultural studies
Phase 3	**Research Strategies** • Case study. • Phenomenology. • Biographical method. • Clinical research.
Phase 4	**Methods of Collection and Analysis** • Interviewing. • Observing. • Artefacts, documents and records. • Visual methods. • Data management methods. • Computer-assisted analysis.
Phase 5	**The Art of Interpretation and Presentation** • Writing as interpretation. • Evaluation.

Source: Adapted from Guba and Lincoln (2005)

The author's thinking is very much constructivist[45] within the post-positivist paradigm.

[45] Posture may be defined as the relationship that the researcher wants to have with the subject (Pereira et al. 2003).

[45] Constructivist epistemology is an epistemological perspective in philosophy about the nature of scientific knowledge. Constructivists maintain that scientific knowledge is constructed by scientists and not discovered from the world. Constructivists claim that the concepts of science are mental constructs proposed in order to explain our sensory experience. Constructivism believes that there is no single valid methodology which means there are multiple methodologies for social science (Taylor and Derrick 2007).

Phase two provides the interpretive paradigms that guide the research and Guba and Lincoln (2005, p.105) go on to provide a summary for each paradigm, reproduced in Table 6 below.

Table 6: Interpretive Paradigms

Paradigm/Theory	Criteria	Type of Narration
Positivist/Post-positivist	Internal, external validity	Scientific report, case studies
Constructivist	Trustworthiness, credibility	Interpretive case studies
Feminist	Lived experience, dialogue, caring , race, class, gender, emotion,	Essays, stories, experimental writing
Cultural studies	Cultural practices, social texts	Cultural theory

Source: Guba and Lincoln (2005)

Other texts provide the researcher with a guide to establishing a suitable posture before embarking on the detailed work ahead. For example, Chenail (2003, p. 14) attempts to simplify these into the four C's:

- Curiosity and qualitative methods
- Confirmation and quantitative methods
- Comparison and comparative methods
- Critiquing and critical methods

The author recognises his research posture as one of curiosity in the context of knowing more about the subject, thus further aligning the research strategy to a qualitative approach.

3.2.2 Qualitative Methods

According to Patton (2002), qualitative research is multi-method in focus, involving a naturalistic approach to its subject matter. Creswell (2003, p. 51) notes the following features of qualitative studies:

1. Field focused.
2. Rely on 'self' as research instrument.
3. Interpretive in character.
4. Rely on the use of expressive language and the presence of voice in the text.
5. Attend to particulars.
6. Believable and instructive because of their coherence and insight.

Mahoney and Goertz (2006) claim that qualitative methods are the best strategy for exploring a new area; a point which is particularly pertinent to the area of operational risk mitigation in the UAE.

Qualitative research is not without its problems. Denzin (2006) describes how critics see qualitative research as being unscientific, only exploratory or entirely personal and full of bias. Citing Patton (2002), Flyvbjerg (2006) identifies a few weaknesses of qualitative research; such as, the inability to manipulate independent variables, and the risk of improper interpretations. A number of authors (Janesick 1998, Gummesson 2000, Yin 2002, Holliday 2007) provide guidance on how such disadvantages may be minimised, if not eliminated. Holliday (2007) points towards using multi-methods or methodological triangulation as one way of overcoming these problems.

Mahoney and Goertz (2006) adopt a pragmatic attitude towards qualitative research, describing it as the precursor to the quantitative study. The qualitative work develops the model and provides a definition of the concept. The quantitative work can then operationalise the variables[46] and measure adherence to the model. In this scenario, both methodologies have an equally important role to play in the development of knowledge. In reflecting on the research that the author undertook, one of the major strengths with a qualitative approach is its openness to opportunistic possibilities that emerge during the period of study. For example, the author was able to witness a change to the risk management structure in one of the banks studied and discuss how this could impact upon operational risk mitigation. In fact, only structural, reporting and responsibility arrangements within the Corporate Risk Management Function were affected.

3.2.3 Quantitative Methods

The quantitative approach focuses on measurement, and is of significant help in validating relationships that may exist (Mahoney and Goertz 2006) and, more importantly indicate direction and strength of causality. Quantitative research uses large sample surveys, or other instruments such as experiments, to gather data and then submits the data to appropriate analysis to prove that the relationship either exits or does not exist, or the hypothesis is confirmed or otherwise.

The author does not believe that using quantitative methods for this research study would have necessarily enhanced the reliability and validity of the research findings. Quantitative

[46] To 'operationalise' a variable means to decide how to measure it (Shields and Hassan 2006).

methods could have been used if operational risk was much better addressed and the study population was large enough to warrant the use of questionnaires. According to CBUAE (2010), the number of UAE commercial banks is quoted as forty six. However, due to the sensitivity of the subject, access to data is difficult; which limits the number of banks willing to be part of the research.

3.2.4 Case Study Methods

Yin (2002) explains a case study as an empirical inquiry that investigates a contemporary phenomenon within its real life context. Case study research investigates pre-defined phenomena but does not involve explicit control or manipulation of variables. The focus is on in-depth understanding of the phenomenon or its context (Flyvbjerg 2001).

Case studies have been described in a number of different ways: exploratory, explanatory and descriptive (Yin 2002 and Rarick 2003); descriptive, illustrative, experimental, exploratory and explanatory (Gerring 2005); intrinsic, instrumental and collective (George and Bennett 2005). Such descriptions, whilst helpful in illustrating the type of case study being undertaken, must be preceded by an understanding of the researcher's epistemology (see section 3.2.1). Soy (2006) reminds researchers that case study research can be used in the positivist and post-positivist traditions, with a single or multiple case study design, using qualitative or mixed methods. Other authors point out that case studies are favoured for answering the 'how' and 'why' research questions (Flyvbjerg 2001, Yin 2002, Dul and Hak 2008).

Citing Yin (2002), Flyvbjerg (2006, p. 219) argues that using case studies as a research strategy is suggested when the following conditions exist:

1. When the form of research question is 'how' or 'why';
2. Where there is no control over the behavioural events;
3. Where the focus of the study is on contemporary events.

Robert (2009, p.63): adds the following 'key characteristics' of case studies:

1. Phenomena are examined in their natural settings;
2. Data is collected by multiple means;
3. One or few entities (person, group or organisation) are examined;
4. The complexity of the unit is studied intensively;
5. Case studies are more suitable for the exploration, classification and model development stages of the knowledge building process – the investigator should have a receptive attitude towards exploration;
6. No experimental controls or manipulations are involved;
7. The investigator may not specify the set of independent and dependent variables;
8. The results derived depend heavily on the integrative powers of the investigator;
9. Changes in site selection and data collection methods can take place during the work progress.

The author believes that the area of study, operational risk, and the research questions within the study satisfy most of the criteria referred to above.

Case studies may be single or multiple in nature. Multiple-case studies can be used for two purposes – model building and replication (Yin 2002). Stake (2005) describes the evidence arising from multiple cases as more compelling and the design is more robust, although he warns that the decision to undertake multiple case studies cannot be taken lightly because of the time commitment and resource required. Echtelt et al. (2006) argue that multiple cases offer the researcher an even deeper understanding of the processes and good picture of reality. Additionally they consider that the multiple case studies add confidence to findings and can strengthen the perception, the validity, and the stability of the findings.

On the other hand, Flyvbjerg (2006) points out that the advantage of large samples is breadth, whereas their problem is one of depth. For the case study, the situation is the reverse; nevertheless, both approaches are relevant for a sound development of social science (Flyvbjerg 2006).

3.2.5 Case Study Methods in Business Research

Case study research has also previously addressed related fields of study. The study of operations management by Gumport (2002) is probably a close fit to the area of operational risk. Put simply, Operational Managers have to manage operations risk, which in turn falls under the umbrella of operational risk. According to Gumport (2002), operations management involves complex interplays of people, technological systems, and organisational and physical processes, most of which change in their nature over time. Operational risk mitigation has been described as involving a complex series of interactions

between people, processes and technology (Andreas 2007). Therefore, there appears to be a strong similarity.

Back to Gumport (2002) who goes on to analyse what he considers to be true Operations Management case studies which have been published in some mainstream operations management journals[47]. The results of the analysis are reproduced in Table 7.

Table 7: Operations Management Case Studies

Methodology	Research Intent			Totals
	Descriptive	Exploratory	Explanatory	
Pure case study	10	36	4	50
Multiple methods	5	6	5	16
Totals	15	42	9	66

Source: Gumport (2002)

The 'Research Intent' is similar to Yin's (2002) terminology as the basis of analysis, thus:

- Descriptive – describes a hitherto unstudied situation.
- Exploratory – focuses on model building.
- Explanatory – involves hypothesis generation.

[47] Journal of Operations Management, International Journal of Operations and Production Management, IEEE Transaction on Engineering Management and International Journal of Production Research.

As can be seen from Table 7, the basis for most of the case studies was exploratory with an emphasis on using a pure case methodology rather than multiple methods to triangulate the results.

3.2.6 Strengths and Weaknesses of Case Studies

Many of the writers on case study methodology have documented the relative strengths and weaknesses of the approach. The reader is reminded that all forms of research have limitations (Yin 2002) and that some of the strengths and weaknesses quoted reflect an argument for or against qualitative research rather than the case study methodology. Table 8 represents a selection of the comments made in the literature reviewed.

Table 8: Strengths and Weaknesses of Case Studies

Analysis of Case Studies	
Strengths	**Weaknesses**
1. Case studies are strong in reality – they are down to earth in details and attention as they report actual behaviour (Gummesson 2000).	1. Case studies rely on analytical generalisations (Flyvbjerg 2001).
2. Case studies are non-disruptive research method – they are in harmony with the reader's own experience (Yin 2002).	2. Case studies can take a long time to complete and result in drowning in the data (Rarick 2003).
3. Case studies recognise the complexity of social truth (Rarick 2003).	3. Case studies lack statistical reliability (there is element of bias) (Zainal 2005).
4. Case studies allow for a large number of variables and different aspects of the phenomenon (George and Bennett 2005).	4. Case study analysis may establish relationships between variables but not necessarily the direction of the causation (Straits and Singleton 2006).
5. Case studies are of high value in the applied social sciences where research often aims to provide practitioners with tools (Stake 2005).	5. Some case studies, for reasons of confidentiality, have to disguise the identity of the organisation(s) being studied (Zahid and Riaz 2008).
6. Multiple case studies add confidence to findings (Echtelt et al. 2006).	6. Case studies represent interpretations of social reality and as such cannot be too objective (Muhamat 2009).
7. Case studies are valuable in developing and refining concepts for further studies (Echtelt et al. 2006).	
8. Case studies offer the opportunity for a holistic view of a process (Primus 2008).	
9. Case studies enable phenomena analysis in their natural settings (Robert 2009).	

Source: Developed by the author

Many of the texts quoted provide counter arguments to the weaknesses. Robert (2009) in particular, provides a robust and detailed defence against the criticisms made. Stake (2005) also discusses mitigating factors and counter arguments, and in particular points to the use of multiple case studies to strengthen or broaden the analytic generalisations as well as the precision, validity, and stability of the findings. It behooves all researchers to recognise the

inherent weaknesses in their approach and then to develop an appropriate research design, which overcomes as fully as possible the shortcomings using a range of tactics, such as, paying attention to details, adhering to the research timeline framework, addressing data bias, using multiple case studies to enhance confidence in the results, and most important of all, validating the results using methodological triangulation (Stake 2005).

3.3 Research Design for This Study

3.3.1 Research Design

Yin (2002) explains the research design as the logic that links the data to be collected and the conclusions to be drawn to the initial questions of the study. He points out that there are elements to consider when determining a research strategy:

1. The type of research question posed;
2. The extent of control an investigator has over actual behavioural events;
3. The degree of focus on contemporary as opposed to historical events.

The answers to these three questions furnish an indication to the type of strategy to be adopted in undertaking the research, as depicted in Table 9.

Table 9: Relevant Situations for Different Research Strategies

Strategy	Form of research question	Requires control over events	Focuses on contemporary events
Experiment	How, Why	Yes	Yes
Survey	Who, what, where, how many, how much	No	Yes
Archival analysis	Who, what, where, how many, how much	No	No
History	How, Why	No	No
Case study	How, Why	No	Yes

Source: Yin (2002)

Using this analysis, the strategies suggested for completing this research were case studies.

Methodological triangulation (section 3.3.3) should enhance the reliability of the results but, as Holliday (2007) notes, a factor that must be considered is the perceived magnitude of the benefits that integrating case study work and survey methods would bring, particularly in relation to assessing the quality of the research design. His view suggests that methodological triangulation could be a judgemental issue, which researchers must be aware of throughout the course of the research project, and should be taken into account during the development of the research proposal. As detailed in section 3.3.3, *Critical Incident Techniques* were used to triangulate the results. Surveys across all the UAE commercial banks to triangulate the results for this study were not used due to access barriers, and since identifying all the individuals within all the UAE commercial banks who could participate in the survey would have been a difficult exercise due to the diverse nature of operational risk and the large number of potential actors involved. On the other hand, a survey of one set of actors, for example, Risk Managers could have been done, but

this would have produced biased results. Further, the four banks selected are major and influential players in the industry. Given this, it is believed that the results from the four case studies are sufficient to answer the research questions.

Bailey (2008) notes that the practical issues of access, availability of secondary data[48], budgets, time pressures and experience of the potential users must also be considered in the research design. Robert (2009) points out that the design and scoping of the research project requires a comprehensive literature analysis to be undertaken in order to understand the existing body of research literature within the research area and to position the research questions within the context of the literature. He also points to other factors that could impact upon the design, including the purpose for which the research was undertaken, the resources available to the researcher and the deliverables required.

The overall design for this study showing the research phases, processes involved and documentation produced is shown in Table 10.

[48] Secondary data is data collected by someone other than the user. Primary data, by contrast, is data collected by the investigator conducting the research (Corti and Bishop 2005).

Table 10: Research Design: Phase/Process/Documentation

Phase	Process	Documentation
1. Literature Review	Define framework/methodology	Literature review write up (Chapter 2)
2. Research Framework	Define strategy/context/ preliminary model Define semi-structured interviews and case study protocol Identify potential cases	Cases for study Research questions (Version 1) Case study protocol (Version 2)
3. Pilot Case Study	Conduct pilot case study Analyse pilot case study	Pilot case documentation Pilot case results
4. Pilot Case Study Review	Refine questionnaire Refine case study protocol	Research questions (Version 2) Case study protocol (Version 2)
5. Multiple Case Studies	Conduct case studies Analyse case study data Evaluate results	Multiple case documentations Multiple case results
6. Critical Incidents	Discuss CIT's Analyse CIT's	Triangulation
7. Model Building	Develop model Refine model	Revised model Model documentation
8. Conclusion	Interpret findings Identify implications	Study implications (chap 5) Implications for further research (chap 6)

Source: Developed by the author

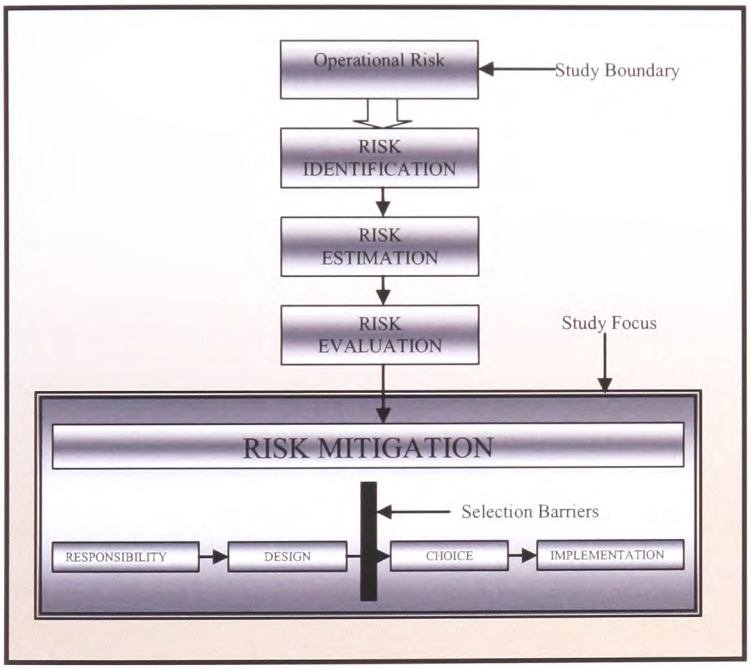
3.3.2 Preliminary Research Model

Thomas and Jaines (2006) argue that a research focus is necessary in order to avoid being overwhelmed in data. They also point out that it is incumbent upon researches using case-based methods to be clear about their initial theoretical propositions, a point supported by Flyvbjerg (2006) who also warns of the dangers of completely disregarding any existing maps of the ground being explored.

It has been argued that risk mitigation involves making decision. Decision-making theories have been explored in the literature in Chapter 2 of this study and it was decided that an

appropriate starting point for this research would be an extension of the risk management model, as applied to operational risk, using the decision making model driven from the literature (see section 2.2.3). This provided the author with the preliminary model for the risk mitigation process in Figure 2, depicted below as Figure 12 for easy reference.

Figure 12: Preliminary Risk Mitigation Model



Source: Developed by the author

Based on the work of Simon (1997) and Lurie (2004) discussed in section 2.2.3, the four risk mitigation phases are described below:

1. Responsibility – who has responsibility for operational risk mitigation (not included in the decision making process)?
2. Design – what tactics are employed to mitigate operational risk exposures?

3. Choice – what is the process for selecting and implementing risk mitigation actions or tactics?
4. Implementation – what follow-up (e.g. reporting) is carried out to ensure that the risk has been effectively mitigated?

The researcher needs also to identify the categories or groups of people that, in combination, can provide both a comprehensive picture of the phenomenon under examination, and a variety of perspectives on that phenomenon (Atkinson et al. 2007). The literature review (Basel II) identified those areas with a primary concern for effective operational risk mitigation as being the Risk Management Unit, Internal Audit and Operational Management themselves. The view points of these three groups were considered important because:

1. The Risk Manager's viewpoint – the Risk Manager plays an integral part in the overall management of risk within the business;
2. The Internal Auditor's viewpoint – the Internal Auditor has an indirect role in mitigating risks through his examination of the internal control systems;
3. The Operational Manager's viewpoint – the Operational Manager acts as the owner of the process within which the risks have to be identified and mitigated.

The reason for selecting these groups is that the preliminary model included all of these groups in the 'responsibility' phase of risk mitigation. There are, however, other groups who - it could be argued that - have secondary concern for operational risk mitigation, such

as external auditors, consultants, outsourcing companies and regulators. By selecting the primary groups, the research data was kept more manageable, and enabled identification of commonalities of approach. Additionally, maintaining an internal bank focus ensured that stronger controls were achieved over the data since external parties would have approached the problem of mitigation from their own agenda.

The reporting of risk mitigation actions in the UAE commercial banks is not present in the literature and the model assumed that there would be some form of reporting so that follow up or tracking could be undertaken to ensure that the risk mitigation action is being or, has been carried out and is working effectively. Such an assumption was justified on the basis of regulatory pressures (Basel II) that would require documentary evidence of risk mitigation actions to be available for inspection, for example, audit reports on control improvements are mandatory actions. The absence of such reporting could be seen as a weakness in the ORM system.

Another important part of the model is shown as selection barriers. It was assumed there would be constraints placed on the organisation/functional units/individuals on what choices can be taken forward to implementation. The author approached the identification of these barriers by probing the interviewees about their views on the selection barriers.

3.3.3 Triangulation

Yin (2002) maintains that triangulation is the application and combination of several research approaches in the same research to validate the results. It can be employed in both

qualitative research modes, including case studies, and quantitative research modes for the purpose of validation.

Creswell (2003) claims that by combining multiple observers, methods, and empirical materials, researchers can overcome the data bias and other problems that may arise from a single methodology strategy. This claim is also supported by other writers (O'Donoghue and Punch 2003, Altrichter et al. 2008).

Stake (2005) identifies four basic types of triangulation:

1. Data triangulation: involves time, space, and persons.
2. Investigator triangulation: involves multiple researchers in an investigation.
3. Theory triangulation: involves using more than one theoretical scheme in the interpretation of the phenomenon.
4. Methodological triangulation: involves using more than one method to gather data.

Triangulation has been employed in this study using *Critical Incident Techniques* (CIT's) to validate the results (Serenko 2006), since CIT's provide data that can be used to either substantiate or reject the data analysis findings concerning operational risk mitigation (see next section). The approach is consistent with the fourth type of triangulation as identified by Stake (2005).

In order to validate the results, and ensure that the findings make sense, the following strategy path has been followed:

1. Triangulation of data sources to validate convergence of findings using CIT's;
2. Multiple-case study strategy has been employed;
3. The findings have been related back to the literature whenever possible (see Chapter 4).

3.3.3.1 Critical Incident Techniques (CIT)

Gremler (2004) explains the Critical Incident Technique as a procedure used for collecting direct observations of human behaviour that have critical significance and meet certain criteria. The observations are then analysed and compared to the research findings. Critical incidents can be gathered in various ways, but typically respondents are asked to tell a story about an experience they have had (Gremler 2004).

Gremler (2004, p. 29) goes on to point out that a CIT is a flexible method that usually relies on five major steps: The first is determining and reviewing the incident, then fact-finding, which involves collecting the details of the incident from the participants. When all of the facts are collected, the next step is to identify the issues, followed by determining how the issues were resolved based on various possible solutions. The final step is the evaluation, which will determine if the solution that was selected would solve the root cause of the incident.

Zach (2004) describes the use of *Critical Incident Techniques* (CIT's) as a way of validating the data analysis results. The idea behind CIT's is to encourage the manager

(unit of analysis, see section 3.3.6.4) to explain an incident (operational risk incident) in some detail and then to illustrate how the incident was eventually overcome (how it was mitigated) and whether it is in line with the data analysis results.

Support for using CIT's is also found in Serenko (2006) who notes that collecting data about such events can portray the organisational processes and enable patterns in the overall data to be identified and compared.

The author is also confident that the use of *Critical Incident Techniques* within the case study approach also helps to overcome some of the problems concerned with comparability of data from the basic units of analysis. This comparability may arise since Risk Managers and Internal Auditors are generally governed by external regulations and professional standards, whereas Operational Managers in different disciplines can have a wide variety of functional responsibility, vested interests, experience and skills.

Hughes (2007, p. 51) defines a critical interview technique as:

> "A qualitative interview procedure which facilitates the investigation of significant occurrences (events, incidents, processes or issues) identified by the respondent, the way they are managed, and the outcomes. The objective is to gain an understanding of the incident from the perspective of the individual."

He sees a critical incident as having the following characteristics:

1. It should contain only one event or chief description;
2. It should identify persons, locations and times as specifically as possible;
3. It should either be observed by the writer or be verifiable by more than one source;

Serenko (2006, p 33) sees a critical incident as having the following advantages:

1. Can be applied using questionnaires or interviews.
2. Identifies events that might be missed by other methods which only focus on common and everyday events.
3. Data is collected from the respondent's perspective and in his or her own words.
4. Does not force the respondents into any given framework.
5. Useful when problems occur but the cause and severity are not known.
6. Provides rich information.

He also places emphasis on making sure that critical incidents are not written in judgemental terms, and do not attempt to summarise too much nor be too general.

Based on the above illustration, CIT's were used during the course of the interviews as data triangulation strategy for the study. This process was accomplished by collecting additional set of data, analysing it, and comparing it to the data analysis results of the main interviews. Sorenko (2006) demonstrates that CIT's provide data that can be used to either substantiate or reject (i.e. validate) the findings (concerning operational risk mitigation).

The questions used to discuss the critical incidents in this study were part of the case study protocol and can be found in *Appendix B1*.

3.3.4 Data Analysis

3.3.4.1 Qualitative Data Analysis

The common qualitative data analysis approaches are examined in this section, and the logic of choosing one approach over another is given.

Yin (2002, Ch. 5) explains data analysis as a process of inspecting, categorising, tabulating and modelling data with the goal of highlighting useful information, suggesting conclusions, supporting decision making and addressing the initial proposition. Creswell (2003) points out that data analysis has multiple approaches, encompassing diverse techniques under a variety of names, in different business and sciences, and it is incumbent upon the researcher to develop a general data analysis strategy as part of the case study data design.

The interpretation of data is recognised as a critical and difficult phase in qualitative research (Lindlof and Taylor 2002) and there are some excellent sources of reference available to the researcher to guide him through the process (see for example Yin 2002, Glaser 2005, Echtelt et al. 2006, Baxter and Jack 2008). There is no one approach of qualitative data analysis, but rather a variety of approaches, related to the different perspectives of the researcher (Glaser 2005). Researchers are also advised that successful qualitative research is entirely dependent upon a constant interaction among the research design, data collection, and data analysis (Echtelt et al. 2006).

Holliday (2007) advocates that the most common analysis approach of qualitative data is observer impression. That is, an expert observer examines the data, interprets and reports the findings in a structured form. He goes on to point out that one of the most important parts of this qualitative data analysis approach is the data de-muddling or careful deliberation that takes place and how the de-muddle of information clears into patterns.

The author recognises Holliday's (2007) approach as allowing the data to speak for itself, and organising the emerging thoughts into a coherent pattern. In order to broaden the reader's knowledge, the following is a cross section of the common qualitative data analysis approaches:

3.3.4.1.1 Content Analysis

Stemler (2001) explains the Content Analysis (CA) approach as compressing many words of text into fewer content categories based on explicit rules of coding. It often involves building a fixed vocabulary of terms and word frequencies. He points out that words and phrases mentioned most often are those reflecting important concerns. Therefore, CA starts with word frequencies.

Klaus (2004) points out that with the rise of computing facilities, computer-based methods of CA are growing in popularity. The input is analysed for frequencies and coded into categories for building up inferences.

Roger (2005) claims that a frequent criticism of CA is that it can only be applied to identify the words, sentences, or texts themselves, rather than their inter-relations. As pointed out earlier, ORM is a complex area where actions are inter-related and inter-dependent. Accordingly, the author would argue that CA is not an optimal choice for data analysis for this study.

3.3.4.1.2 Discourse Analysis

Harris (1991) explains Discourse Analysis (DA) as an approach to analysing written, spoken or signed language use. He points out that DA has been taken up in a variety of social science disciplines, each of which is subject to its own assumptions, dimensions of analysis, and methodologies.

Schiffrin et al. (2001) point out that the objects of DA (writing, talking, conversation, communicative event) are variously defined in terms of coherent sequences of sentences, propositions or speech acts. According to Johnstone (2002) DA does not only study language use beyond the sentence boundary, but also prefers to analyse naturally occurring language use.

In DA, formal equivalence relations among the sentences of a coherent discourse are made explicit by using sentence transformations to convert the text into a basic form. Words and sentences with equivalent information are then grouped together. The work is then progressed into a fully articulated informational content and invoked into a system for computer-aided analysis (Blommaert 2005).

An inherent limitation in DA is to decide when a particular piece of information (data) is relevant to the topic being researched (Gee 2005). Considering the complexity of ORM, all parts of interview data is considered relevant and needs to be conceptualised. Accordingly, the author would contend that DA is not an optimal choice for data analysis for this study.

3.3.4.1.3 Recursive Abstraction

Stebbins (2001) explains Recursive Abstraction (RA) as an approach to analysing qualitative data without coding, where data is summarised; the summaries are then further summarised, and so on. The end result is a more compact summary that would have been difficult to formulate without the preceding steps of distillation.

Fischer (2005) points out that a frequent criticism of RA is that the final conclusions are several times removed from the underlying data. He counters this criticism by claiming that analysts need to document the reasoning behind each summary step, citing examples from the data where statements were included and where statements were excluded from the intermediate summary. Considering the complexity of ORM, all conclusions from the data are considered important and need to be maintained. Accordingly, the author would argue that RA is not an optimal choice for data analysis for this study.

3.3.4.1.4 Grounded Theory

According to Allan (2003), Grounded Theory (GT) is a qualitative research methodology that emphasises generation of theory from data in the process of conducting research. He goes on to point out that it is a research method that operates almost in a reverse fashion from traditional research and at first may appear to be in contradiction with the scientific method. This point is picked up by Glaser (2005) who advocates that rather than beginning by researching and developing a hypothesis, the first step is data collection. From the data collected, the key points are marked with a series of codes, which are extracted from the text. The codes are grouped into similar concepts in order to make them more workable. From these concepts, categories are formed, which are the basis for the creation of a theory, or a reverse engineered hypothesis Glaser (2005).

Since generating a new hypothesis is not part of the study objectives, the author would contend that the GT qualitative data approach is not the optimal choice for data analysis for this study.

3.3.4.2 Coding

According to Marshall and Rossman (1998), Coding is an interpretive technique that both organises the data and provides a means to introduce its interpretations. They go on to explain that most coding requires the analyst to read the data and demarcate segments within it. Each segment is labelled with a word or short phrase 'code.' When coding is complete, the analyst prepares reports via a mix of summarising the prevalence of codes,

discussing similarities and differences in related codes across distinct original contexts, or comparing the relationship between codes.

Contemporary qualitative data analyses are sometimes supported by computer programmes. These programmes do not limit the interpretive nature of coding but rather are aimed at enhancing the analyst's efficiency at data analysis, storage and retrieval and at applying the codes to the data (Patton 2002).

Lindlof and Taylor (2002) point out that a frequent criticism of coding method is that it seeks to transform qualitative data into quantitative data, thereby draining the data of its variety, richness, and individual character. They counter this criticism by advising analysts to thoroughly expose their definitions of codes and link those codes soundly to the underlying data, therein bringing back the richness that might be absent from a mere list of codes.

Citing Lindlof and Taylor (2002), Holliday (2007, p. 53) points out that irrespective of the data analysis approach, the data analysis process boils down to three main flows of activity:

1. Data reduction: The process of selecting, focusing, simplifying, abstracting, and transforming the data that is collected during field work;
2. Data display: Organising, compressing, and assembling the information to permit conclusion drawing and action;
3. Conclusion drawing and verification: Noting regularities, patterns, explanations, possible configurations, casual flows and propositions.

Holliday (2007) indicates that these three themes are interwoven and provide a well-established framework to undertake a thorough qualitative analysis of the captured data. (Holliday 2007) supports the view of Weik (1995) by emphasising that data analysis under this framework becomes an iterative process which means that the process is repeated again and again, using the results from the previous stage

The author followed the advice of Holliday (2007) in his qualitative data analysis approach. Written data from transcripts were conceptualised line by line. A process of going back and forth while comparing data, constantly modifying, and sharpening the growing conclusions was employed (see also section 3.3.4.1).

In order to facilitate the process, the data was coded based upon the best practices suggested by a number of authors (see Patton 2002, Denzin and Lincoln 2005, Charmaz 2006) in order to find out relevant patterns.

The coding system was based upon the preliminary research model and enabled a structured approach to be taken from the beginning of the data analysis. The coding was revised after the pilot case study had been completed. The final version is presented in *Appendix B2* as part of the case study protocol.

Computer software, ATLAS.ti, was used to facilitate data analysis and provide a repository of the data that could be collected and stored electronically, thus forming part of the case study database.

Thomas and James (2006) warn about drowning in data and being unable to distinguish the most significant parts from those peculiar to a particular case, something which is easy to do when a big variety of data sources exists. How much data to collect and analyse is a judgemental matter which must consider how much additional data would help to validate the research approach and results. They reiterate that the experience and skills of the researcher play an important part in this process. Serenko (2006) captures an important innate or natural ability relating to the human psyche; thus, human beings are born with the ability to absorb a vast amount of information and make sense and order of that information. A view that was in fact supported by Mey and Mruck (2007) who claim that people are meaning-finders; they can very quickly make sense of most chaotic events.

3.3.4.3 Drawing Conclusions

The ability to draw valid conclusions rests in the hands of the researcher; and his skills and experience are tested to the extreme at this stage of the process. Several texts describe the qualities of a good researcher (Clarke 2005, Thomas and James 2006, Mey and Mruck 2007). The researcher is in fact the research pillar, as it is he or she who is at the centre of the research process and who drives the whole effort forward. Based on their many years of experience in the field, Mey and Mruck (2007) believe that a knowledgeable researcher with conceptual interests and more than one disciplinary perspective is often a better

research instrument for qualitative research, as he is more refined, more bias resistant, more economical, quicker to 'home in' on the core processes that hold the case together, and more persistent in the search for conceptual meaning.

Whatever the researcher's skill base is, there are still a number of issues that must be considered in assessing the quality of the conclusions drawn from the research study. Such issues are described by Mey and Mruck (2007) and are related to this study in Table 11.

Table 11: Issues in Assessing the Quality of the Research Conclusions

Issue	Method used in the study
Objectivity/Confirmability Relates to the extent of relative neutrality and freedom form researcher bias.	1. The general methods and procedures have been fully described and critiqued; 2. The data collection and analysis is fully auditable enabling repetition of the study.
Reliability/dependability Relates to the issue of quality control over the study.	1. The research design is congruent with the research questions; 2. The basic paradigms and beliefs are articulated and related to theory; 3. A monthly supervisory reporting mechanism was established at the outset of the study.
Authenticity Do the findings of the study make sense?	1. Triangulation of data sources produced convergent findings; 2. A multiple-case study strategy used; 3. Findings were related back to the literature whenever possible.
External Validity//Fittingness Relates to the generalisability of the results.	1. The study focused on major commercial banks in the UAE market; 2. Critical incidents and other published operational risk incidents support the findings.
Utilisation/Application/Action Orientation Relates to the pragmatic validity of the results in the research/practitioner's community.	1. The study results are important to a number of stakeholders, for example, regulators, shareholders, Board and Senior Managers; 2. An operational risk mitigation checklist has been developed; 3. A high level audit overview document for reviewing the work of the Operational Risk Function has been produced.

Source: Developed by the author (based on Mey and Mruck (2007))

3.3.5 Quality of the Research Design

Yin (2002, p. 33) identifies four common tests for judging the quality of research design:

1. Construct validity: establishing correct research procedural measures.
2. Internal validity (for explanatory studies only, and not for descriptive or exploratory studies): establishing a causal relationship, whereby certain conditions are shown to lead to other conditions.
3. External validity: establishing the domain to which a study's findings can be generalised.
4. Reliability: demonstrating that the operations of a study, such as the data collection procedures can be repeated, with the same results.

It has been stated that this research is exploratory and the author was, therefore, concerned with ensuring the research design had construct validity, external validity and reliability.

Yin (2002) provides guidance on tactics that may be used (and the phase within the research process) to ensure such conditions are met. Table 12 provides further details.

Table 12: Case Study Tactics for Four Design Tests

Tests	Case Study Tactic	Phase of Research in Which Tactics Occur
Construct validity	- use multiple sources of evidence/triangulate - establish chain of evidence - have key information review - draft case study report	Data collection Data collection Composition Composition
Internal validity (not applicable to this study)	- do explanation building - do time-series analysis	Data analysis Data analysis
External validity	- use replication in multiple case studies	Research design
Reliability	- use case study protocol - develop case study data base	Data collection Data collection

Source: Yin (2002)

In the context of this research study, the author followed Yin (2002) and has employed all suggested tactics. The use of critical incidents was seen as an effective way of providing evidence about the theoretical territory within which the study was bounded, thus enhancing construct validity. Further, multiple sources of evidence (see section 3.3.6.6), key information review and drafting case study reports were employed for this purpose. External validity which indicates that the findings can be generalised from companies in the sample to other companies or industries (Mitchell and Jolley 2001) is, of course, a matter of degree since no empirical study can offer certainty that its findings are valid for other populations (Shadish 2002). In this study, however, it is anticipated that the results will be generalisable to other sectors of the UAE financial services industry, such as insurance companies, since their operations are similar and many UAE commercial banks are known to have insurance subsidiaries. The issue of reliability and, in particular the reliability of interview data, is of concern in any case research. The goal of reliability is to minimise the errors and biases in a study (Yin 2002). Yin goes on to suggest that a good guideline is to conduct the research so that an auditor could repeat the procedures and

arrive at the same results. The author considers his background, and the need to develop properly documented files, create sufficient evidence to support the findings and present them in such a way that a verifiable audit trial can be created, is of considerable help in satisfying this particular element. The development of a case study protocol (section 3.3.7) further helps to satisfy this requirement.

3.3.6 Selection for the Cases Studied: The Way Forward

3.3.6.1 Pilot Case Study

Yin (2002) advocates that a pilot case study helps investigators to refine their data collection plans with respect to both content of data and the procedures to be followed. Straits and Singleton (2006) describe a pilot case study as being exploratory, enabling problems and issues to be identified which may point to further investigation. The author believes that the objective of a pilot case study is, therefore, to provide the researcher with a solid foundation such that the research process is in tune with the reality of the situation in the field. The research began with a detailed pilot case study, which aimed to confirm this position and provide the author with feedback concerning the development of the final case study protocol. The bank selected for the pilot was chosen on the basis of the author's personal knowledge of the concerned employees and ease of access.

3.3.6.2 Sampling

Lawrence (2006) refers to sampling as the process of collecting information from a population. He classifies sampling methods as: 'random/probability' (random sampling,

systematic sampling, stratified sampling, cluster sampling) or non-random/non-probability (convenience sampling, purposive sampling, snowball sampling). The most common reason for sampling is to obtain information about a population, since sampling is quicker and cheaper than a complete census of a population (Firebaugh 2008).

The number of cases used in the research was determined using the following criteria:

- The inherent difficulties in gaining access and discussing in detail a new area where sensitive information could, and indeed was, disclosed during the interviews and probing of critical incidents;
- The fact that any further case studies would have only marginally contributed to a better response to the research questions since the four selected banks are major players in the UAE commercial banking industry. If the results from the four selected banks had been divergent, the 'reserve' banks identified in the case study protocol would have been contacted and further work done.

Scholz and Tietje (2002) discuss the issue of how many cases are needed. They discuss the emphasis placed on numbers as being important but not a paramount issue; because although the number of studies conducted is important, no investigation can be defined on the basis of that issue alone. Rarick (2003) points out that there is no ideal number, whilst Straits and Singleton (2006) suggest that between two and ten cases are desirable. This study has used four for the reasons noted above.

Practicalities played an important part in selecting the number of cases studied. There was a need at the outset to identify commercial banks that were known to have an ORM function. This type of approach is referred to as purposive sampling where the objective is to choose sources that will help to answer the basic research questions and fit the basic purpose of the study (George and Bennett 2005, Lawrence 2006). Random or representative sampling is not preferred in this type of environment due to difficulties in gaining access to sensitive information, as pointed out above.

3.3.6.3 Study Population

Chapter 1, section 1.1.4 has already described the logic behind selecting the UAE commercial banks as the study population.

The UAE commercial banks represent a homogeneous and discrete group although they may differ in terms of size and business focus. They are all, however, regulated by the same body (CBUAE) and will, therefore, be required to maintain sound standards of operation in their business activities, including risk management. Additionally, it was anticipated that they would have a range of operational risk problems to manage.

Yin (2002) advises that when multiple-case studies are used, each case must be carefully selected so that it either predicts similar results (literal replication) or produces contrasting results but for predictable reasons (theoretical replication). Theoretical replication involves selecting cases due to suspected intrinsic differences between them Yin (2002), and it is required to make general statements about the differences and similarities (see section 4.6).

(Creswell 2003) points out that when only a few cases (two to five) are selected, then literal replication, or selecting cases so that they are likely to predict similar results is appropriate. The author therefore selected the cases bearing this in mind.

Another element to consider is the bounding of the case study (Cash and William 2002) or deciding what is included and what is excluded. The author of this thesis argues that exercising control over the boundaries can be difficult with large organisations, which may themselves contain a number of business units that could, on their own, be bounded as a case study. In the case of the UAE commercial banks, they are known to operate in other market sectors such as insurance. This study was bounded at the organisational level and not confined to any particular business unit.

To summarise, the selection criteria for the sample chosen was based on what has been discussed and on a number of factors including how well established the bank was, how successful (in terms of profit, reputation, and so on) the bank had been, the information in the public domain about the bank's risk management policies and the information in the public domain concerning operational risk problems in the bank. It was hoped that by adopting these criteria the selected banks would recognise the relevance of the research to their own organisation thus facilitating access. Researchers would work with organisations and identify what is in it for them, according to Robert (2009). The author hoped from the outset that the research study would be of interest to the UAE commercial banks since operational risk and the development of appropriate methodologies to manage operational risk are of topical interest in this sector of business.

3.3.6.4 Unit of Analysis

Yin (2002) provides guidance on selecting the unit of analysis. He explains the unit of analysis as being related to the way the initial research questions have been defined. Typical units of analysis include the individual, the organisation or even the society itself. The unit of analysis in this study is the manager, i.e. person interviewed, within the bank since it is his interaction with the operational risk mitigation process that is the focus of the study. Whilst this study is concerned with how the organisation mitigates operational risk, it is at the level of the individual that the mitigation action is formulated.

Selecting a function within the banks as the unit of analysis was not possible because the managers selected came from a variety of departments and business units, and to restate, the focus of the study was on how the organisation, and not how a certain function, mitigates operational risk.

3.3.6.5 The Research Instrument

The research instrument is the tool that enables the researcher to obtain responses to his questions from the respondents (Yin 2002). Lindlof and Taylor (2002) explain the semi-structured interview as a qualitative research tool commonly employed in qualitative research. They point out that a semi-structured interview is flexible and allows new questions to be brought up during the interview as a result of what the interviewee says, and allows face-to-face interaction to take place enabling the author, for example, to see

how long respondents took to answer a particular question when some thinking time was required (barriers to mitigating operational risk). This ensures that answers can be reliably aggregated and that comparisons can be made with confidence between sample subgroups or between different survey periods (Lindlof and Taylor 2002).

The interviewer in a semi-structured interview generally has a framework of themes to be explored (Kvale and Brinkman 2008). However, this does not preclude prompting the interviewees with additional questions when the context dictates (Kvale and Brinkman 2008).

Considering the fact that, for this research, the purpose of the interview questions was to direct the interview and allow the interviewee to elaborate on his views (Joubish 2009) on operational risk, the semi-structured interview approach was selected as the appropriate research instrument.

3.3.6.6 Data Collection

Hentschel (1998) points out that for qualitative methods, researchers can revert to in-depth interviews, direct observation and written documents for data collection. Furthermore, Shah and Corley (2006) maintain that qualitative methods for data collection and analysis can be powerful, especially in an area that is not well researched. Their view supports the author's approach to research operational risk mitigation in the UAE commercial banking industry using qualitative methods for data collection and analysis

Yin (2002, p.80) lists six sources of evidence without reference to their relative strengths and weaknesses:

1. Documentation – such as letters, memoranda, internal reports, annual reports, press reports, minutes of meetings or emails.
2. Archival records – such as organisational charts, personnel records, internal magazines or internal material.
3. Interviews – structured or semi-structured.
4. Direct observation – via field visits to the sites.
5. Participant observation – where the researcher takes an active role in the case.
6. Physical artefacts – such as technological devices, a work of art, trophies or photographs.

Flyvbjerg (2006) considers that no single source has a complete advantage over the others; rather, they might be complementary and could be used in tandem, and most case studies have one or two sources of data as the primary collection vehicle. The goal is to obtain a rich set of data surrounding the research issues, as well as capturing the contextual complexity (Kvale and Brinkman 2008), but collecting case study data from case participants alone can be difficult and time-consuming (Robert 2009).

The main data collection source used in this study was a semi-structured interview designed to elicit information from the selected managers about ORM and, in particular, the mitigation process. The author noted the comments of Serenko (2006) concerning the

disadvantages of taped interviews; such as, the respondent being sometimes self-conscious or overly aware of the recorder, and the equipment may malfunction. In response, each interviewee was given the option of having the interview taped, and the author had a spare machine available at all the interviews. Each interview was transcribed and the transcript sent to the interviewee for verification, correction and reflection vis-à-vis the responses given. The author concluded each interview with a statement ensuring that lines of communication remained open. In some cases follow-up questions were raised by the author to clarify issues that had been discussed during the interviews.

The questionnaire was developed by the author as part of the case study protocol. It was subject to revision after the pilot case study had been undertaken. The final document is part of the case study protocol (*Appendix B1*). The use of a preliminary model for the operational risk mitigation process enabled the author to specify the potential factors and discuss them at the interviews. Data could thus be organised in a systematic way which aided subsequent analysis. Secondary data pertinent to the banks was collected by the author during the field work and from the internet. Such data includes annual reports, internal reports, power-point presentations, organisational charts and press reports.

The interviews were also the most appropriate method for collecting data about the critical incidents cited by the managers. Gremler (2004) notes that the *Critical Incident Technique* is a method for coming close to direct observation, but avoids some of the hardships. Serenko (2006) goes on to point out that the method allows more incidents and mini-cases, to be collected than would be possible through direct observation.

The overall data collection method enabled a good level of data triangulation using CIT's to be achieved in the study, one of the important criteria for construct validity.

3.3.6.7 Organisational Confidentiality

Robert (2009) points out that there are two key points to be addressed in order to gain the cooperation of interviewees: confidentiality and benefits to organisations. The author was aware of the need for confidentiality given the sensitive nature of the subject matter and provided assurance both to the banks involved and the interviewees that their confidence and trust would be respected. The managers interviewed needed to be assured that the information given, particularly when discussing critical incidents, would not affect, for example, the researcher's views of the banks.

Data collected from the critical incidents was in some cases extremely sensitive. Obtaining approval from the companies took a considerable effort according to Zaugg (2006) in his case study research into 'On-line complaint Management.' The author knew from the outset that gaining access was one of the major risks of the study. Operational risk incidents within the UAE commercial banking sector have occurred regularly throughout the course of this study as press reports attest to (see for example Gulfnews, Sept.16, 2008 issue). Access was gained through a variety of channels following which an initial meeting was set up to discuss the aims and objectives of the research project, whom needed to be interviewed and the likely duration of the interviews. The author had made contingency

plans if access was not granted (see section 3.3.7.4), and in the event only one bank in the original list of four declined[49] the invitation to participate.

None of the banks or the managers interviewed has been named (see tables 13 and 14) and no interview quotes have been attributed. Each bank is referred to using a Greek letter; however, the bank names and reports were made available to the researcher's supervisors.

3.3.7 Case Study Protocol

Yin (2002) suggests that a detailed case study protocol is desirable under all circumstances, but is essential if a multiple case study design is used. He further advocates that a protocol helps to focus the research and provide a framework within which the case study may be carried out. The author followed the case study protocol developed by Straits and Singleton (2006), which they believe enhances the reliability and validity of the investigation. The following is an overview of the case study protocol developed for this study.

3.3.7.1 Project Objectives

The overall objective of the project was to examine one aspect of the ORM, namely risk mitigation, in the context of one type of business risk, namely operational risk, within the UAE commercial banking industry. This led to the development of the research main and secondary questions (section 1.2.3).

[49] The invitation was declined because the bank was going through some significant organisational changes including a review of the operational risk management function.

3.3.7.2 Background Information

A literature review of the operational risk area had been produced highlighting the scarcity or lack of previous academic research in the area of operational risk in the UAE commercial banking industry. Other areas of risk management have been examined in some detail, for example, market risk and the application of VaR methodologies to calculating market risk exposures. However, ORM (in the context of commercial banking industry in the UAE) has only recently attracted attention following the CBUAE mandate that the UAE commercial banks ensure that they fully adhere to Basel II operational risk recommendations by 1st Jan. 2011, and the Financial Crises. The result is that there are some challenging opportunities to further build a model in the operational risk area. The preliminary risk mitigation model was drawn from the decision-making theory which has been well researched and developed from an academic standpoint.

3.3.7.3 Summary of the Substantive Issues

The rational for selecting the UAE commercial banking was based on the literature review undertaken as a prelude to completing the research proposal (section 1.1.4). This highlighted the growth in operational risk exposures being experienced by the UAE commercial banks generally resulting from factors such as globalisation, business climate, regulatory pressures and the Financial Crises. Whilst operational risk is a feature of many businesses, there is increasing pressure on the banking sector to ensure that adequate ORM procedures are in place. It was expected that the UAE commercial banks, in particular,

would have a range of operational risk problems and, as such, represent a suitable group upon which to examine the research question. One of the expected outcomes of the research was the establishment of the practices within the selected population of the UAE commercial banks. The risk mitigation phase of ORM was chosen as the focus of the research (although it was recognised that the other phases would need to be addressed) since it could be seen as representing one of the most important daily challenges facing management, i.e. how best to reduce the operational risk exposures identified. The research questions were examined by using a series of probing interviews with key players in ORM in the selected banks. These interviews were semi-structured and a template of the questions was developed to guide the process (*Appendix B1*).

3.3.7.4 Structure of the Field Procedures

- **Banks chosen for the study** - The list of banks chosen for this study is shown in Table 13.

Table 13: Lists of Banks Chosen for the Study

Bank	Location	Contact for gaining access
Alpha	UAE	Head of Operational Risk
Beta	UAE	Head of Operational Risk
Gamma	UAE	Head of Operational Risk
Delta	UAE	Head of Operational Risk
Bank A (declined)	UAE	Head of Operational Risk
Bank B (reserve)	UAE	Head of Operational Risk
Bank C (reserve)	UAE	Head of Operational Risk
Bank D (reserve)	UAE	Head of Operational Risk
Bank E (reserve)	UAE	Head of Operational Risk

Source: Developed by the author

The initial list of banks was selected because they were known to represent main players in the UAE commercial banking. They were, therefore, likely to have an Operational Risk Unit and an Internal Audit department. The selected banks were approached directly (by telephone) by the author as the first step to gaining access. This was followed up by a letter enclosing a copy of the condensed research proposal. A follow up visit was made to arrange an interview when face-to-face discussions could begin.

- **Determining the people interviewed** - Serenko (2006) discusses the selection of respondents when interviews are to be used to collect data, and suggests that they should be chosen on the basis of what the researcher desires to know and from whose perspective that information is desired (see section 3.3.6.4 for a discussion on selecting the manager as the unit of analysis).

Further, the author was aware from the literature review (Basel II) that, in particular, the key actors in ORM were the Risk Management Function, Operations Management in the various business units and Internal Audit. For each of the banks involved, initial contact was made with the Head of Operational Risk[50]. The final interviewee choice was left to the Head of Operational Risk. Table 14 shows the positions of the people interviewed (generic titles have been used, however, the real titles were made available to the supervisors) for each of the banks involved in the study and where in the organisational structure they were positioned. Factors taken

[50] This is a generic title and represents the most senior person responsible for the Corporate Operational Risk Function.

into account in the selection criteria included managers from separate businesses, managers who have experienced recent operational risk problems (in order that *Critical Incident Techniques* could be employed at the interviews), managers with long auditing experience and Operational Risk Managers working in the business units.

Table 14: Managers Interviewed

Bank	Person Interviewed	Functional Area
Alpha	Director of Risk Management	Corporate Risk Function
	Head of Operational Risk	Corporate Risk Function
	Director of Internal Audit	Corporate Internal Audit Function
	Operations Manager	Treasury Business Unit
	Security Manager	IT Business Unit
Beta	Head of Operational Risk	Corporate Risk Function
	Operational Risk Manager	Treasury Business Unit
	Director of Internal Audit	Corporate Internal Audit Function
	Operations Manager	Retail Banking Business Unit
Gamma	Head of Operational Risk	Corporate Risk Function
	Head of Business Risk	Corporate Risk Function
	Director of Internal Audit	Corporate Internal Audit Function
	Operational Risk Manager	Corporate Banking Business Unit
	Operational Risk Manager	IT Business Unit
Delta	Head of Operational Risk	Corporate Risk Function
	Head of Risk Finance	Corporate Risk Function
	Director of Internal Audit	Corporate Internal Audit Function
	Internal Audit Manager	Treasury Business Unit
	Operational Risk Manager	Finance Business unit

Source: Developed by the author

The pilot and main interviews were held during the year 2010, most averaged three hours each and were conducted according to the interviewees' schedules and availability as suggested by Kvale and Brinkman (2008).

- **Access issues** - The author's personal contacts within the banking sector helped to gain access to data and only one of the original banks would not participate (due to impeding organisational changes). The sensitivity of the information gathered during the study is recognised and all material has been personally controlled by the author. All the information collected during the project has been maintained in a series of protected project files, which included data collected from the case studies.
- **Contingency plans** – In case of difficulties in gaining access, the author made a number of contingency arrangements to move the study forward (see Table 13).
- **Resources used** – the author personally carried out all the interview work in order to maintain a consistent approach throughout. Transcribing of the taped interviews and all the subsequent data analysis was carried out by the author. Case study work was reviewed on an ongoing basis by the supervisor in order to ensure that the work carried out met the high academic standards of professionalism demanded at doctoral level.

3.3.7.5 Case Study Questions

- **The nature of the questions** – case study questions can be classified into three groupings as detailed below (see *Appendix B1*). It is important to structure the interview questions according to the sequence of risk mitigation events and the author utilised the risk management model to help structure the interview. In order

to avoid the issue of bias, the questions were not shown to the interviewees. The principal reason for developing case study questions was to provide a tool for data collection and subsequent data analysis.

Group 1 questions – relate to bank's ORM details. Those in large type represented primary questions, whilst those in smaller type were likely to be answered during the discussion of the primary question and are, therefore, secondary questions.

Group 2 questions – relate to the critical incidents across the cases.

Group 3 questions – relate to the Financial Crisis and Dubai Crisis.

3.3.7.6 The Analysis Plan

Outline of the case study report – for each of the case studies undertaken a case study report was prepared. Preparing an initial outline of the report before the field work began helped to focus the author on the main topics to be covered and also provided an aid to structuring the work. The reports are presented in *Appendix B3* as part of the case study protocol. A draft of the report was sent to the bank for commenting and corroboration of the validity of the findings.

- **Database of evidence** – an important element of any case study work is the evidence that is accumulated during the field work. Such evidence was maintained in a database for subsequent use and analysis where appropriate. The transcripts of the interviews form a key part of this database as they are the main source of data. Other data collected before, during and after the field work (for example relevant

information from the Annual Report and the website) has been included in the data base.

- **Transcription and coding of data** – following the transcription of the interviews, a coding system was used to provide a first cut analysis of the data. The coding system used was based on the research questions and the theoretical framework and was focused on the area of operational risk mitigation. A preliminary code list was prepared before detailed work had begun and amended in light of the experience gained during the pilot case study. *Appendix B2* illustrates the high level coding used.
- **Statistical analysis of data** – the software package, ATLAS.ti was used to help analyse the data. This is a well-developed qualitative data analysis tool which was used to draw meaningful conclusions and develop emerging themes from the fieldwork results (section 3.3.4.2).
- **Interpretation of results** – following the data analysis, the results were examined for consistency across case studies in order that valid overall conclusions could be drawn (section 3.3.4.3).

3.3.8 Limitations of the Research Design and Mitigation Strategies

3.3.8.1 Limitations and Mitigation Strategies

By concentrating on the UAE commercial banks, there are a number of limitations built into the research. Table 15 documents the possible limitations and illustrates the strategies adopted to mitigate the effect of these limitations.

Table 15: Limitations of the Research Design

Possible Limitation	Mitigation Strategy
1. The results of a single industry study may not be generalisable to other business sectors within the financial services or other countries.	The selected banks operate in a number of sectors within financial services and have overseas operations.
2. The selected managers may themselves be biased in their approach to operational risk mitigation and may not necessarily be representative of the bank as a whole; giving rise to data bias.	The semi-structured interview was designed to cover all aspects of the operational risk mitigation process and not just a focus on one area.
3. There may be an element of 'group-speak' in the way the managers responded to the interview questions.	This rests to a certain extent on the skill of the interviewer and the need to be vigilant when conducting the interview. The probing of a critical incident avoided, in particular, any possibilities of 'group-speak.'
4. There is uncertainty about the 'adoption' of clear definition of operational risk and the categories within it.	The opening part of the semi-structured interview focused on establishing whether Basel II definition was adopted and whether the respondent understood it.
5. There is a possibility that the banks chosen for the case study purposes may not provide a good representation of the industry as a whole.	The selected banks were chosen because they are key players in the UAE commercial banking industry.
6. The design of the interview questions may reflect the author's personal bias.	The development of the questions was based on the generic ORM framework established from the literature review and was subject to revision after the pilot study.
7. Interview questions can be interpreted in different ways and the responses may be prone to exaggeration.	Various sources of data are available to support the key responses and data analysis has concentrated on identifying key themes.

Source: Developed by the author

3.3.8.2 Data Bias and Mitigation Strategies

Bias is a personal and sometimes unreasoned judgement which takes place in human communication. It needs to be avoided in order to have accurate research results and to uphold research standards and professional ethics (Shah and Corley 2006).

The researcher anticipated moderate bias scenarios such as biased interviewees and group-speech, and projected suitable mitigation tactics. Such bias scenarios were mitigated by ensuring that the semi-structured interview was designed to cover all aspects of the operational risk mitigation process and not just a focus on one area, and the vigilance to

remain neutral and consistent exercised by the researcher when conducting the interview (Calvet 2007).

Calvet (2007) points to the availability of a wide spectrum of tactics to counteract data bias, such as avoiding suggesting answers, avoiding steering the survey in a way that pleases the researcher, avoiding body language or expressions that indicate the researcher's feelings about the respondent or the answers, and extending neutral reinforcement when necessary. The researcher endeavoured to use these tactics when and as needed throughout the research.

This section has focused on the research options available to the researcher and the actual research design used in this study. Case study methods have been selected as they offer the best opportunity to answer the research questions. The use of case studies was reviewed and appraised and the research design highlights the focus on critical incidents as a means of data triangulation. The research design was assessed and critiqued and strategies for overcoming the limitations were identified.

4. STUDY FINDINGS

4.1 Introduction

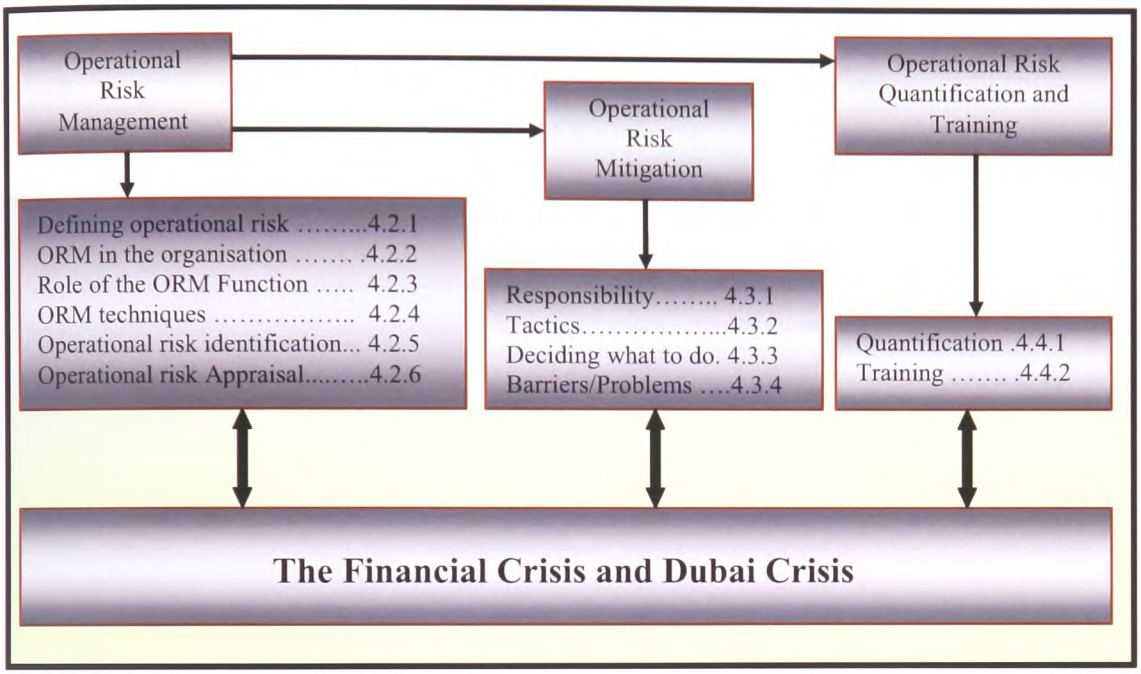
This Chapter provides analysis of the results of the data collected from the case studies.

The Chapter is split into seven parts:

1. Operational risk management (section 4.2) – discusses the findings related to the operational risk environment and the pre-mitigation phases;
2. Operational risk mitigation (section 4.3) – discusses the findings related to the principal research area and provides answers to the related research questions;
3. Operational risk quantification and training (section 4.4) – discusses the findings related to two areas of operational risk that are important elements of an overall operational risk management strategy;
4. Operational risk and the Financial Crises (section 4.5) – discusses the findings related to the operational risks contributing to the Financial Crises, their impact and how they were mitigated in the context of the UAE commercial banks.
5. Case summaries (section 4.6) – discusses the common themes and differences between the banks based on the cross-case analysis.
6. Critical incidents (section 4.7) – discusses the application of critical incidents to validate the data analysis results.
7. Summary (section 4.8) – provides a summary of the Chapter.

The sequential flow of parts 1 – 4 of this Chapter is shown in Figure 13.

Figure 13: Sequential Flow of Research Findings



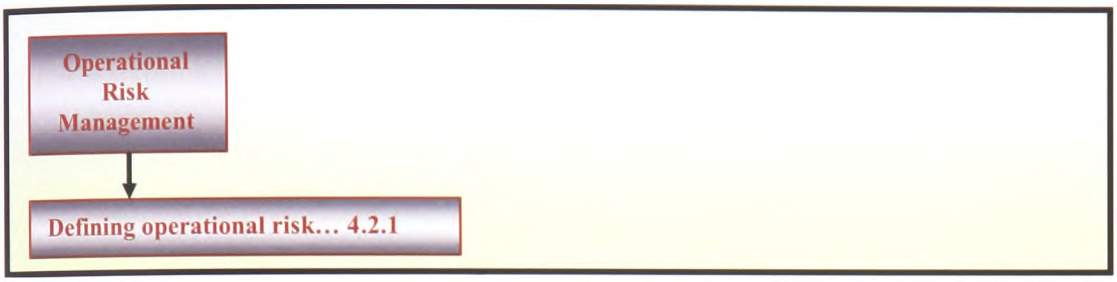
Source: Developed by the author

This diagram provides a roadmap for this Chapter of the thesis and the part under discussion of the diagram will be included at the beginning of each sub-section to help the reader follow the sequence of the findings.

The reader should be aware of one important point before examining the rest of the Chapter. Delta bank was implementing its operational risk framework during the time the author engaged with them. The author was aware of this when they were chosen and selected them on the basis that they represented a newcomer to the field and would, therefore, bring a different perception to the phenomenon (Atkinson et al. 2007).

4.2 Operational Risk Management

4.2.1 Defining Operational Risk



It has been previously illustrated that operational risk is a broad area encompassing a range of risks that typically fall outside of the market, credit, strategic and reputational risk areas. This definition of operational risk has certainly been adopted by many organisations (Moosa 2007, Dorfman et al. 2008, Hubbard and Douglas 2009). The four banks in this study had, however, adopted Basel II definition of operational risk; with minor variations in some cases to accommodate specific bank requirements. Table 16 illustrates this point and provides further analysis relating to the definition.

Table 16: Definition of Operational Risk

Definition of Operational Risk	ALPHA	BETA	GAMMA	DELTA
Source of definition	Adapted Basel II[51]	Adapted Basel II[52]	Basel II	Basel II
Specific risk exclusions	Market, credit	Market, credit	Market, credit, strategic, reputational	Market, credit, strategic, reputational
Level of understanding	Good	Good	Good	Good

Source: Analysis of survey data

[51] The Basel definition had been adopted by the end of the study.

[52] The Basel definition had been adopted by the end of the study.

The Basel II definition used by two of the banks was cited in 1.1.3 and is re-stated here for completeness and easy reference:

"Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk" (Basel II, p. 140).

The other two definitions were:

"Operational risk is the exposure to financial or other damage arising through failure in the Group's operational processes/systems."

"Operational Risk is the risk that deficiencies in information systems or internal controls will result in unexpected loss. The risk is associated with human error, system failures and inadequate procedures and controls."

These definitions are similar, although they do not explicitly refer to external events as being a source of potential operational risk. Evidence[53] from these two banks does, however, support the notion that such events are included.

One Head of Operational Risk described how he has two definitions of operational risk, one which is used from a purely 'measurement perspective' and the other quoted above

[53] Specifically, Alpha bank has external events on its high level risk schedule and Beta bank has external risks as an operational risk category.

from a 'responsibility perspective'. This particular Operational Risk Unit is in the process of developing its approach to operational risk quantification (or measurement).

All managers (Table 16) were aware of their bank's definition and agreed that it described their own understanding of operational risk. As one interviewee put it:

> "It is as good as it can be when you try to be concise about something which is so large."

The research found that the exclusion of strategic and reputational risks under the umbrella of operational risk was not consistent across the banks. The precise definition of strategic risk was not discussed although it was broadly seen as risks relating to the strategies being adopted by the bank. Alpha bank provided the most interesting analysis of this area as the author noted differences of opinion within the organisation. One Alpha bank manager believed that strategic risk could feed into operational risk when, for example a particularly high growth risky strategy was being adopted, thus creating new risks and affecting the impact and probabilities of existing ones. A similar argument was used by another Alpha bank manager in the context of environmental risk, which does fall within the definition.

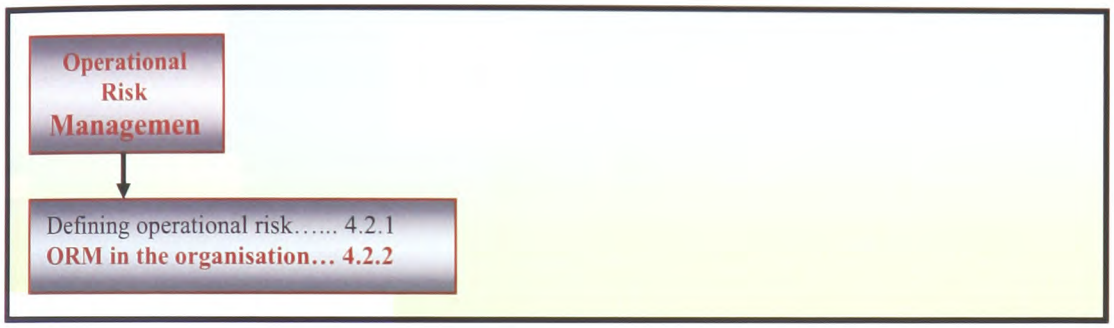
> "You could use a set of words to describe environmental risk in a way that it could be seen as an operational risk, but you could also see it as a credit risk. For example, if you've got contaminated land with a commercial loan, people walk away from the site, that is a credit risk, but you can also think of ways that environmental risks can be translated into operational risk."

4.2.1.1 Main Findings

The finding are consistent with the previous observations in the literature review to defining operational risk: there is a generally accepted definition (Basel II) and whilst all

banks exclude market and credit risk, certain other types, in this case strategic and reputational may or may not be excluded. All managers were aware of their bank's definition and agreed that it described their own understanding of operational risk.

4.2.2 Operational Risk Management in the Organisation



This section examines the organisational arrangements for ORM within the case studies. Table 17 provides the findings of the analysis.

Table 17: Operational Risk Management Functions in the Organisation

Organisation	ALPHA	BETA	GAMMA	DELTA
Corporate OR unit reporting lines	Group Risk	Group Risk	Group Risk	Group Risk
Internal Audit reporting lines	Group Risk	Deputy CEO	Group Risk	Group Risk
Relationship: OR vs. Internal Audit	Very close	Close	Close	Close
Size of Corporate OR Unit	5 persons	6 persons	4 persons	3 persons
Establishment of Corporate OR Unit	2008	2006	2008	2009
Use of Business Unit ORM	Developing 4 Persons	Developing[54] 3 Persons	Well developed 6 persons	Just started 2 Persons
Business Unit ORM reporting lines	Local Management	Local Management[55]	Local Management	Local Management[56]
Relationship: Business Unit ORM vs. Corporate OR unit	Close	Close	Close	Close
OR Committee	No	Part of risk committee	Yes, several	Yes, one
Other OR roles	None	None	Part time risk officers	None

Source: Analysis of survey data

The research found that the establishment of a Corporate Operational Risk Function was a relatively recent phenomenon. One of the units had been established several years ago, two had just been established when this research study started and one was established during the research study. This finding is important because it confirms the relative newness of explicit operational risk management in the UAE commercial banks and further supports

[54] This was developed by the end of the study.
[55] Reporting to the Corporate Operational Risk Unit was introduced towards the end of the study.
[56] Reporting to the Corporate Operational Risk Unit was introduced towards the end of the study.

the methodological approach undertaken. Some of the reasons given for the creation of these units were:

> "CBUAE requirement."

> "...grew out of the need to separate a role which combined operational risk, business continuity planning, corporate governance and one or two odd jobs."

> "...greater recognition that we suffered 'incidents'...that were not credit or market risk by nature."

> "...provide more of a 'front end focus' to operational risk management, i.e. what could happen to the business if we take this decision?"

The use of local Operational Risk Managers in the Business Units is at different stages of development in the banks. Gamma bank had six at the time of interviews, together with some risk officers[57], whilst Delta had two (one of whom was doing the role on a part-time basis) but were in the process of appointing more. None of the local Operational Risk Managers reported to the Corporate Operational Risk Function although they had close links and maintained regular contact. All the local Operational Risk Managers interviewed stressed that they were part of the Business unit:

> "...my role is to facilitate the business units to be able to address operational risk and give them the tools to do so."

> "...mentor and coach on all matters relating to operational risk in the Business Unit."

[57] The risk officer was only part-time in the sense that the individual had other responsibilities

All of the Corporate Operational Risk Units reported up through the Group Risk line, ultimately to a Group Risk Director or Chief Risk Officer (CRO). In all but one of the banks the Internal Audit function had a similar reporting line. This is an interesting finding because it leaves open the question as to how the Internal Audit function can independently review the work of the Corporate Operational Risk Unit if they both report to the same executive. The relationship between the Corporate Operational Risk Unit and Internal Audit has been assessed by the author in subjective terms and is seen as very close at one bank and close at the other three. Alpha bank, where the relationship was judged to be very close, initially established its operational risk unit within Internal Audit before separating the two. This links into another interesting finding: in all of the banks, at least one person working in the area of operational risk had an Internal Audit background. This could have influenced the development of the working relationship, although there were other comments, which indicated a relative proximity of the objectives of the two functions:

> "...operational risk framework helps the business to define what its policy towards operational risk should be... ...Internal Audit's role is to stand outside of the corporate governance framework and look in at it and actually give an overall level of assurance to the Board at the end of the day that all those things that have been created by management, including the operational risk framework, are actually an effective set of controls."

> "Internal Audit is there to be a monitor of the actual implementation of operational risk management framework and the effectiveness of the controls that sit in that environment."

> "We meet regularly. I don't think there are any issues. There is always the concern of overlap, but I'm quite clear about the distinction."

The development of an Operational Risk Committee was, in some cases, more advanced than others amongst the banks. It was outside the scope of this research to examine the role and effectiveness of operational risk committees and how they may be structured to provide the most effective contribution to the ORM framework.

4.2.2.1 Main Findings

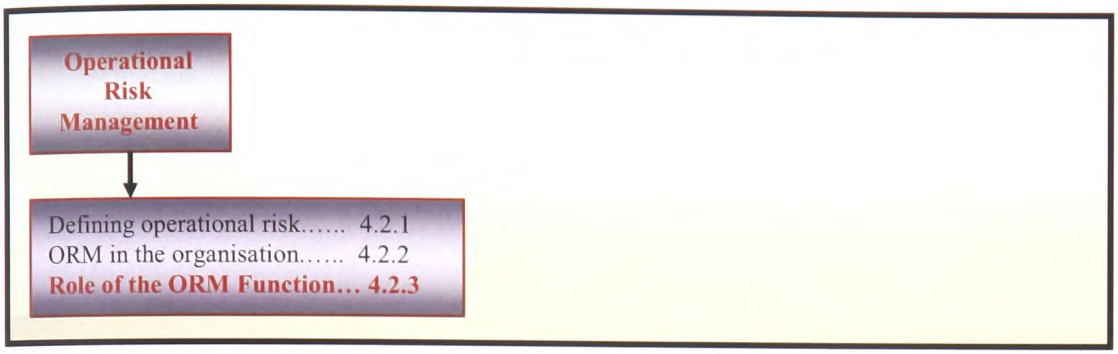
The research found that establishment of a Corporate Operational Risk Function was a relatively recent phenomenon, which again confirms the relative newness of explicit ORM in the UAE commercial banks.

The development of Operational Risk Committees was, in some banks, more advanced than others. Given the relative newness of the Operational Risk Function, it suggests that this is an area that will continue to evolve.

The use of local operational risk managers in the Business Units was at different stages of development in all of the banks.

All of the Corporate Operational Risk Units reported to a Group Risk Director or Chief Risk Officer (CRO). Internal Audit function had a similar reporting line in most of the banks. There is a close relationship between the Corporate Operational Risk Unit and Internal Audit.

4.2.3 The Role of the Operational Risk Management Function



This section concentrates on the role of the Corporate Operational Risk Function. The previous section discussed how the organisation of ORM had developed with two specific roles: the Corporate Operational Risk Manager and the Business Unit or local Operational Risk Manager. The early analysis of the data highlighted that whilst both have a role to play in the overall risk management framework; the corporate function was the driver behind the policy and overall strategic direction of ORM. The Business Unit Operational Risk Managers operate at the 'sharp end' and are much more involved in the day-to-day management of operational risk.

The results of the data analysis in this area indicate that there is a reasonable degree of commonality amongst the banks in the general role that the Corporate Operational Risk Function undertakes (see Table 18). Whilst this might initially seem somewhat surprising given that the creation of these departments is relatively recent, it may reflect the developments that have taken place in other risk (principally market and credit) areas within the bank, which are believed to be more mature. It may also be that managers

involved in the establishment of the ORM function had discussions (at an informal level) as the generic problems they face in managing operational risk are similar across the banks.

Table 18: Role of the Corporate Operational Risk Functions

Role of Corporate Operational Risk Function	ALPHA	BETA	GAMMA	DELTA
Policy setting	Yes	Yes	Yes	Yes
Monitoring function	Implicit in role	Yes	Yes	Yes
Scope of role	All operational risks	All operational risks	All operational risks	All operational risks except environmental risk [58]
Custodians of the framework	Yes	Yes	Yes	Yes
Assurance on 'key' risks	Yes	Yes	Implicit in role	Yes
Aggregating OR's	Yes	Yes	Yes	Yes
Mitigating OR's which span the Business Unit	Coordinate effort	Coordinate effort	No	No
Maintenance of loss data base	Yes	Yes	Yes	No[59]
Corporate Operational Risk Unit works with Business Unit ORM	Often	Often	Very often	Developing
Corporate Operational Risk Unit works with Business Units	Often	Often	Occasionally	Developing

Source: Analysis of survey data

A number of managers captured concisely the role of the function:

> "...to act as a catalyst, to provide a framework, a process, facilitation, to gain people's appreciation that operational risk exists."

[58] By the end of the study, environmental risk had been included in the scope of the role.

[59] Work had begun on this by the end of the study.

> "...embedding risk management culture in the business units so they all become much more risk aware on an everyday basis."

> "...giving these Operational Risk Managers as much guidance and support and general mentoring as to what it is we expect of them, how they should do their work to the best effect, and how they should in turn interact with the business in a positive way and be seen to be helpful and adding value rather than burden that the business has to bear."

The scope of the role was expected to be all operational risks as prescribed in the relevant definition. This was the case in all of the banks with the exception of Delta bank where environmental risks were managed in another area for what appeared to be partly historical reasons (the operational risk function grew out of a unit that originally included environmental risks) and partly due to the emphasis which the bank placed on managing this particular risk.

Different business units have different risk profiles and aggregating these profiles at the group level was done by all of the Group Operational Risk Functions. This aggregation of all the risks should provide the clearest vision of where the key operational risks in the organisation may be found. This is an important finding because it illustrates how the Corporate Operational Risk Function acts as a conduit between the Board and the various Business Units on significant operational risk matters. Their independence from the Business Unit enables this to be done in an objective fashion.

The mitigation of operational risks that span the Business Units[60] was in two cases coordinated by the Corporate Operational Risk Function. Some managers described it as "coordinating mitigation where it's economic to do so." The specific responsibility for these types of risk activities would lie with a specialist area (e.g. IT Security) or another Business Unit (e.g. Personnel) and the Corporate Operational Risk Function would act as the interface with these units ensuring that the mitigation actions were in place. The other two banks operated a different model: one had other specialist risk areas in Group risk that picked them up; the remaining bank used the hierarchical Business Unit structure to escalate such risks to a level where they could be managed. This is an interesting finding because it highlights specific differences of approach to mitigating operational risk that span the Business Units, suggesting that operational risk mitigation has still to mature in some areas.

Emphasis on the maintenance of operational loss data bases (Basel II) occurred earlier to commencement of the research. Excluding Delta bank, evidence was found to support the notion that the maintenance of these databases is undertaken by the Corporate Operational Risk Functions. This finding is consistent with the description of the roles of the Corporate Operational Risk Function that have appeared in the literature review (Coleman 2007).

The interface between the Corporate Operational Risk Function and the Business Units also revealed differences of approach. In Gamma bank, very close liaison existed amongst operational risk personnel both at the Corporate and Business Unit levels. This has been a

[60] Examples of such risks include business continuity, misuse of the internet and loss of key staff.

deliberate strategy and reflects the needs of the Corporate Operational Risk Function to work through the Business Unit Operational Risk Managers if they are to discharge their responsibilities. As Delta bank was piloting the implementation of their operational risk framework, the interface was still developing although evidence seen concerning the roles and responsibilities suggest that they will operate on a similar basis to Alpha and Beta banks.

Evidence drawn from the cases suggests that the core responsibilities of the Corporate Operational Risk Function are as follows:

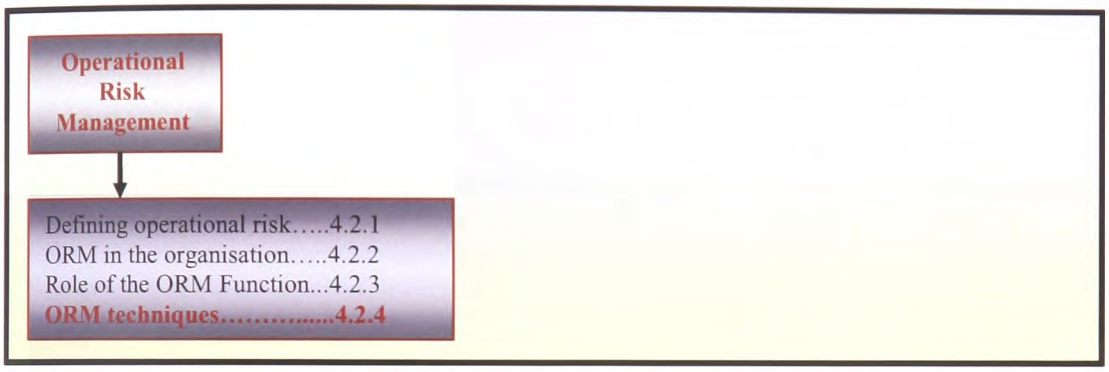
1. Policy: establishing operational risk policy;
2. Aggregation: providing a 'portfolio' view of the operational risks in the group;
3. Reporting: high level reporting of operational risk;
4. Assurance: monitoring levels of operational risk and providing assurance that key operational risks are being managed;
5. Framework: providing the Business Units with the right tools and techniques to manage operational risk;
6. Measurement: developing the techniques for quantifying operational risk.
7. Loss data: maintenance of loss data base.

4.2.3.1 Main Findings

The results of the data analysis indicate that there is a reasonable degree of commonality amongst the banks in the general role that the Corporate Operational Risk Function undertakes. The core responsibilities of the Corporate Operational Risk Function are:

policy setting, aggregation of operational risk profile, high level reporting, assurance, framework setting, operational risk measurement and loss data maintenance.

4.2.4 Operational Risk Management Techniques



In all of the banks studied a form of operational risk mapping technique was being used. The end result of the risk mapping process is a 'register of risks' although the objective was seen to be much broader than just this:

> "One of the things that obviously we're trying to drive forward with this risk management framework is implementing a risk culture. This is different from having a risk process. I think what a lot of organisations have traditionally done as far as operational risk is concerned is they have created these centralised units which are stuffed up with, don't get me wrong, fairly good and knowledgeable people, but they are divorced from the business."

> "We aim to enable businesses to do business according to the terms that they find acceptable. It is not about precluding people from doing business; it is enabling them to do business within a safer environment. So, if you think of it in terms of walking out into the water they can actually go in deeper and take more risk than they might otherwise have done, but they are ultimately safer than they would have done because they have gone through a conscious process of evaluating and determining what is acceptable and what are the controls and what is the other criteria they wish to put round it."

> "Our risk-mapping framework actually covers a number of areas which credit and market risks do not tend to cover, such as research and development, looking at

how organisational structures might be out of place, communication on operational risk issues."

The risk framework was the principal tool used to manage operational risk and was built around the generic management process model identified in the literature review. Table 19 provides further analysis of the data.

Table 19: Operational Risk Management Techniques

ORM techniques	ALPHA	BETA	GAMMA	DELTA
Framework in place	Yes	Yes	Yes	Pilot stage
Type of approach	Top down and Bottom up	Bottom up	Bottom up	Bottom up
Extent of coverage	50% completed	One cycle completed	One cycle completed	Pilot stage
Manage significant project	Several processes	Framework	Separate process	Framework
Loss database	Yes	Yes	Yes	No[61]
Key risk indicators (KRI's)	Yes	Yes	Yes	Yes

Source: Analysis of survey data

Three of the banks use a framework based on a 'bottom up'[62] approach. The exception to this was Alpha bank, whose approach was initially 'top down', as it began with discussions with the Business Unit Management about the key risks that most concern them in running their operation (identification process). This was followed by workshops with the operations staff to determine the other exposure to key risks identified by Management.

[61] Work had begun on this part by the end of the study.
[62] The term 'bottom up' implies the risk process is driven from the lowest level in the organisation and the results are filtered up to executive management.

Any additional risk would also be picked up at this stage. This finding suggests that the starting point may be different but the desired end result is the same. The author undertook further analysis in this area examining the actual data output from the process in order to establish similarities as well as differences. The results are shown in Table 20.

Table 20: Risk Mapping Frameworks – Data Output

Framework – Data Output	ALPHA	BETA	GAMMA	DELTA
Business Unit				
Objectives	No	Yes	Yes	Yes
Materiality threshold	Yes	Yes	Yes	Yes
Identification				
Risk – description	Yes	Yes	No	No
Risk – event/cause	No	No	Yes	Yes
Risk category	Yes	Yes	Yes	No
Recording whether the risk has been experienced	Yes	Yes	Yes	No
Assessment				
Likelihood	Yes	Yes	Yes	Yes
Financial impact	Yes	Yes	Yes	Yes
Consequential impact	Yes	Yes	No	Yes
Mitigation				
Assessment of controls in place	Yes	Yes	Yes	Yes
Indicators to monitor	Yes	Yes	Yes	Yes
Action plans	Not formal	Not formal	Yes	No
Implementation date	No	Yes	Yes	No

Source: Analysis of primary data documents

Further differences are apparent which indicate that whilst the process follows the ORM process model, there are matters of detail that differ resulting from the different emphasis that a particular bank places on the phase in the process. This finding is interesting because

it would appear to demonstrate that banks still have opportunities to refine and possibly improve their risk mapping approaches.

A further finding that emerged during the study was the extent to which the risk mapping process had been implemented within the bank (see Table 19). As has been previously mentioned, Delta bank was piloting the process and still has some way to go before the whole bank has been subjected to the framework. Alpha bank had completed around 50% of the process whilst both Beta and Gamma had done at least one complete cycle.
The risk management of significant change projects[63] was covered by all of the banks (see Table 19). Processes were in place to assess project risks; some of them being fairly recent developments resulting from the introduction of the operational risk framework.

> "We have recognised that there is a need to give a particular focus to that area of business because I think it is an area that has been perhaps not as well recognised or as well identified or as well managed than it has been in the past. But we regard the project risk process as very much a subset of the operational risk mapping exercise as a whole."

The final piece of analysis in Table 19 highlights the common use of key risk indicators to monitor operational risk in all banks and the use of incident loss data bases in all but one of the banks (although Delta bank indicated it was developing one). Key risk indicators were seen as an important feature in the ongoing monitoring of operational risk. One manager described how the use of such indicators would move managers out of their 'comfort zones' when it came to mapping operational risk as they would have to be more proactive in taking action when indicators were moving in the wrong direction. This finding is

[63] There is no definition of what constitutes a 'significant' project but new product developments was mentioned a number of times.

important because the use of key risk indicators to monitor operational risk is a key issue in preventing the manifestation of operational risk.

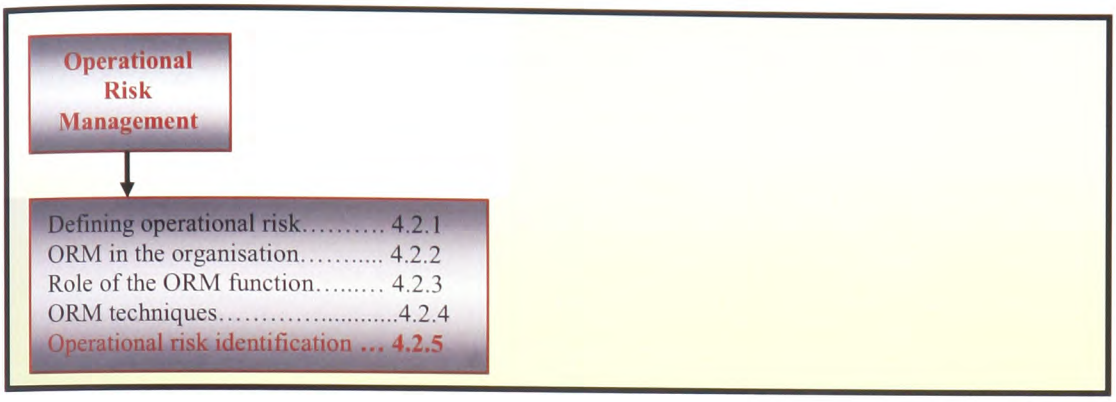
The operational loss data base has taken on a new importance since banks were invited to contribute to an anonymous pooling of data on risk incidents (Basel II, ORX Association 2010). The findings suggest that the banks view this as an important ORM tool.

4.2.4.1 Main Findings

The results of the data analysis indicate that all of the banks use a form of operational risk mapping framework, and in most of them, the framework is based on the 'bottom up' approach. The framework is the principal tool used to manage operational risk and is built around the generic management process model identified in the literature review.

All of the banks use key risk indicators to monitor operational risk, and most of the banks use incident loss databases in order to be more proactive in taking action before an operational risk manifests itself. Key risk indicators and loss database are seen as important ORM tools.

4.2.5 Operational Risk Identification



Operational risk identification has been described as perceiving hazards, identifying failures, recognising adverse consequences (White 1995, Parker 2005). It is the first stage in the ORM process. An analysis of the data revealed that the risk identification process can be split into three phases:

1. Responsibility: Who is responsible for identifying operational risk?
2. Process: What processes are used to identify operational risk?
3. Data: What data sources are used to identify operational risk?

The results of the data analysis are shown in Table 21.

Table 21: Operational Risk Identification: Data Analysis

Operational Risk Identification	ALPHA	BETA	GAMMA	DELTA
Responsibility	Business Unit	Business Unit	Business Unit	Business Unit
Support	When required	When required	When required	When required
Focus	Management concerns	Business Unit objectives	Management concerns, BU objectives and processes	Business Unit objectives
Instrument	Framework	Framework	Framework	Framework
Process	Workshop Material events Networking Software Scenario analysis. Risk indicators IA process	Workshop Material events Project Product development. Internal forums Questionnaires Risk indicators Networking Software Scenario analysis. IA process	Workshop Material events Project/Product development. Software IA process Risk indicators	Workshop Material events Project/Product development. Interviews Meetings Risk indicators Questionnaires External monitor Strategic plan Software IA process
Data source	People Internal loss data Specialised organisations.	People Internal loss data Specialised organisations.	People Internal loss data Specialised organisations.	People
Output	List of risks	List of risks	List of risks	List of risks

Source: Analysis of survey data

Responsibility: The initial discussions that took place in this area concerned the responsibility for operational risk identification, and as Table 21 illustrates there was a common view that this responsibility rested with the 'people who manage the processes

and systems' or the managers in the Business Unit. One manager pointed out how the framework had been developed in such a way to highlight who must take responsibility:

> "Operational risk identification is a business unit responsibility. It doesn't matter how you divide it within your business unit or whom you give it to. That's one of the things we're doing with the methodology."

It was, however, pointed out in all of the banks that other units do get involved in their various specialist roles, for example, Internal Audit was seen as key to helping identify operational risk by "matching the risks with the systems of internal control and where there are weaknesses reporting them." This they do as part of their audits of the various Business Units. This finding supports the view of Basel II and others that the responsibility for ORM, and therefore, identification of operational risks lies with the Managers within the Business Units. Furthermore, according to Basel II, to the extent that the audit function is involved in oversight of the ORM framework, the Board should ensure that the independence of the audit function is maintained. This independence may be compromised if the audit function is directly involved in the ORM process. The audit function may provide valuable input to those responsible for ORM, but should not have direct ORM responsibilities.

One interviewee pointed out that this responsibility is effectively delegated down from the Board that is ultimately accountable for risk management in the organisation. This is in line with the view of Spira and Page (2003) and Basel II.

Process: The process of risk identification does not take place in a vacuum and results of the analysis indicate that for three of the banks the initial focus is the Business Unit objectives.

> "Each business unit is asked during its risk assessment to identify what it feels to be the key risks, the ones that are most important to it in terms of failing to achieve its objectives."

The starting point for Alpha bank was slightly different in that the process begins with a discussion with the directors and Senior Management in the Business Unit on what they consider to be the risks that most concern them. Materiality emerges as a key word in the risk identification process for all of the banks. "Trivial risks", as they were referred to by one bank, may be captured but are not seen as the key focus. This is particularly interesting finding because it illustrates how the processes of identifying and appraising the operational risks are done simultaneously, i.e. managers in identifying their operational risks are also assessing them as 'key' or otherwise. The risk-mapping framework described in section 4.2.4 is used to capture this data.

The processes mentioned by the managers that were used to identify operational risk are quoted in Table 21. The most common, used in all of the banks, are workshops, scenario analysis, KRI's and the Internal Audit process. The workshops can involve a number of different people including Operational Managers, Operational Risk Managers, Internal Auditors and specialists. The Internal Auditors interviewed confirmed that they used a risk

based unit approach[64] (McNamee 1997, Krishnamoorthy 2002). A number of other processes were mentioned but perhaps the most interesting one (mentioned in two of the banks) is networking, both internally and externally. Whereas the other approaches mentioned tend to be more formal and structured, however, networking is more informal:

> "I wouldn't say it was a structured thing. It definitely works as an informal thing."

> "We do rely to an extent on our network of contacts."

Three out of the four banks mentioned the product development process in the context of operational risk identification. Such a process is seen as key in the Treasury function because of the potential financial impact that an operational risk could have. The only bank where the product development process was not mentioned was Alpha. It does, however, have a well-defined and documented product approach, which includes a risk management activity.

All four banks have recently deployed a form of operational risk software application. However, none of the banks is utilising the application as intended. The application in all banks is mainly used for loss data storage and retrieval. Never the less, operational risk software applications can be utilised for a multitude of activities such as (Ciborra 2009, p. 41):

- Integration of the processes pertaining to: risk assessments, internal audits, compliance initiatives and corporate governance.

[64] Instead of looking at the business process in a system of internal control, the internal auditor views the business process in an environment of risk (McNamee 1997).

- Risk analysis and tracking.
- Key risk indicator early warning.
- Reporting on risk.
- Monitoring evolving risk profiles in real-time by centralising data in one risk library.
- Risk communication and training.

The findings indicate that a number of formal processes exist to identify operational risks. Other processes mentioned appear to supplement and support the core processes. These formal processes combined with the informal networking processes provide a wide range of opportunities for operational risk to be captured and the fact that a number of different processes are used supports the argument that operational risk is broad and diverse in nature.

These findings must also be viewed against the current background of ORM which, it has already been confirmed, is still developing in UAE commercial banks. It may be that as the ORM processes mature, the focus of operational risk identification will change. At present, the use of KRI's and workshops serves to capture new risks and re-assess any old ones. A growing trend is to use frequent monitoring of potential operational risk sources and scenario analysis to capture any new risks and to assess existing ones. In future, the use of Software applications, combined external and internal loss data and intensive training, are also likely to have a leading role in this part of ORM.

Data: The research found that the main data source used to identify operational risks was the skill and experience of the people involved in the identification process. Where these people are bank employees, they represent probably the most valuable asset that the banks have in both identifying and managing operational risks. One manager pointed out the importance of having a 'varied skill base' particularly where the project/product development process was involved in examining a new operational risk situation.

> "If you are looking at a fairly mature area, then you probably do not need anything much more than the people who are actually working there who understood the process, because they will have a good understanding of what they are dealing with. If you're talking about a new venture, then I think it's very different because what we are trying to do is brainstorm what the things that might be potential risks are."

Table 21 also shows that three of the banks use their incident loss database as a data source for identifying operational risk. The database currently captures only internal events within the Business Units. These events, however, can be shared across other Business Units to establish whether they have been identified and assessed correctly. This finding illustrates the importance of people in operational risk identification and, as a consequence, the inherent subjectivity that they will bring into the process. Another source of data was circulars by specialised organisations (such as ORX Association). This source is of extreme importance due to the fact it provides up-to-date real data on losses, amounts, frequency and related sources of operational risk.

4.2.5.1 Main Findings

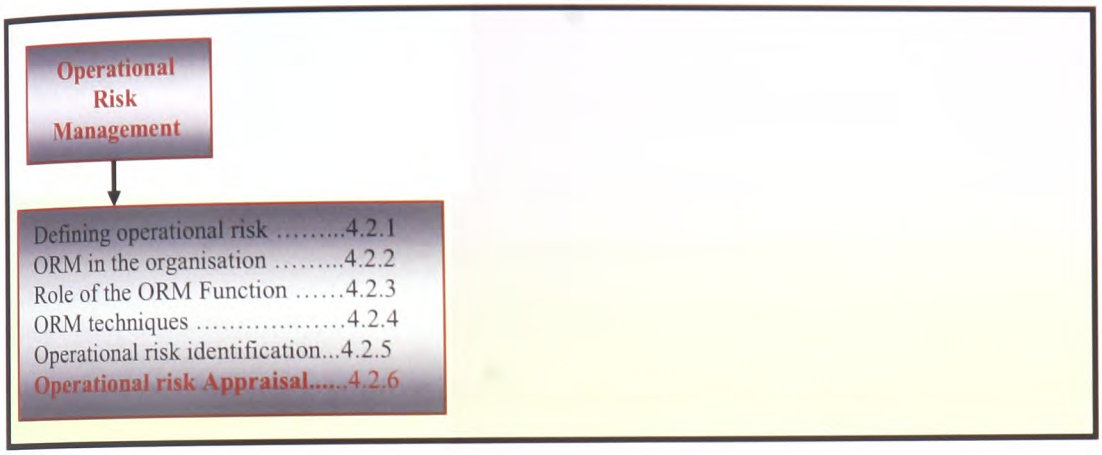
Analysis of the data revealed that the risk identification process can be split into three phases: responsibility, process and data.

Responsibility: The responsibility for operational risk identification rests with the people who manage the processes and systems. The Internal Audit function may provide valuable input to those responsible for ORM, but does not have direct ORM responsibilities.

Process: The findings indicate that a number of core processes (such as workshops, KRI's and networking) exist to identify operational risks. The processes of identifying and appraising the operational risks are done simultaneously. The analysis also indicates that for most of the banks, the initial focus for operational risk identification is the Business Unit objectives. A growing trend is to use frequent monitoring and scenario analysis of potential operational risk sources.

Data: The research found that the main data sources used to identify operational risks were the skill and experience of the people involved in the identification process, incident loss database and circulars by specialised organisations.

4.2.6 Operational Risk Appraisal



The risk management process model identifies the two phases following identification as evaluation and estimation. These two phases have been identified by White (1995) and Parker (2005) in almost similar ways as:

- Estimation: Estimating risk probabilities, describing the risk, quantifying the risk;
- Evaluation: Estimating the impact of the risk, judging acceptability of the risk, comparing risks against benefits.

Following the pilot case study it was noted that these two phases were being done concurrently, and not sequentially as suggested in the model. The output from each phase had a different emphasis with one focusing on probabilities (estimation) and the other on at least financial impact (evaluation) but the two were combined to give an overall risk profile. The author has, therefore, grouped these two phases together and referred to it as 'Risk Appraisal.'

As with operational risk identification, analysis of the data revealed that the risk appraisal process can be split into three phases:

1. Responsibility: Who is responsible for appraising operational risk?
2. Process: What processes are used to appraise operational risk?
3. Data: What data sources are used to appraise operational risk?

The results of the data analysis are shown in Table 22.

Table 22: Operational Risk Appraisal: Data Analysis

Operational Risk Appraisal	Alpha	Beta	Gamma	Delta
Responsibility	Business Unit	Business Unit Corporate Operational Risk Function	Business Unit Corporate Operational Risk Function: (health-check)	Business Unit
Support **Instrument** **Process**	When required Framework Workshop	When required Framework Workshop IA process: challenging	When required Framework Workshop IA process: challenging Operational risk (health-check)	When required Framework Workshop
Likelihood focus **Impact focus**	Probability: 1 - 5 scale AED 1 to 5 scale with 6 scenarios	Probability:% AED: figure	Probability:1 - 5 scale AED: 1 - 6 scale Probability > AED1m: 1 - 4 scale	Probability:1 - 6 scale AED: No. of ranges Consequential impact
Data sources	People Current mitigants Historical data External environment Software Specialised organisations.	People Current mitigants Historical data Specialised organisations.	People Current mitigants Loss Database Risk indicators Software Specialised organisations.	People Current mitigants Performance indicators Specialised organisations.
Output	BU Risk profile Risk measures	Risk rating	Risk rating on a scale of 1 - 8	Risk report

Source: Analysis of survey data

Responsibility: The results in Table 22 show that the responsibility for operational risk appraisal mirrors that of operational risk identification. The Managers in the Business Units have the responsibility for appraising operational risk although they may be aided by specialist resource when the situation demands so. One manager in Beta bank, however, pointed out that in his view, Business Unit Managers had a 'lesser responsibility' and were influenced by the Corporate Operational Risk Function who acted as facilitators to this process using the standards and parameters (for appraising operational risk) that are agreed by the Board:

> "...this is where I see the Operational Risk Group has helped to facilitate operational risk appraisal. Just as the Market Risk Group facilitates Value at Risk, and Credit Risk Group tries to somehow put a number on credit risk. However, it's more difficult for operational risk and I've got a lot of sympathy for that."

This finding probably reflects the framework within which the Business Units are 'obliged' to operate, although a manager in one of the other banks (Delta) considered that there was still some way to go in terms of ensuring that the Business Units clearly understood their responsibility:

> "You'll find sometimes that the Business Unit Managers consider that the Corporate Operational Risk Function has responsibility for some of these things, when in reality they don't. This is because they need the business knowledge to know what the level of exposure is in order to know the level of mitigation needed."

To further reinforce the role that the Corporate Operational Risk Function plays in this area, within Gamma bank they have specific responsibility for performing a 'health-check' on the results for any irregularities or apparent contradictions.

The findings in this area suggest that whilst the primary responsibility appears to be well articulated, the Corporate Operational Risk Function is more influential in the results that are produced. This may be a reflection of the subjective and judgemental nature of the appraisal process (discussed in the next section) and the need to have some form of control over the results.

Process: In all of the banks the process used to appraise operational risks involved a subjective or judgemental assessment of the probability and impact of the risk, primarily through the workshops.

> "It is our experienced people who often help in the assessment of the probability and impact of risk within the workshops."

> "There are some gradings on the risk assessment form that we have and then we also ask them to assess what the likelihood of the risk occurring at that level would be, again bandings from very low up to very high. Using the combination of those two factors we then produce a risk rating on that. It's basically a two dimensional matrix, with the intention of giving the likelihood and the potential financial impact as a rating of how crucial that risk is if you like."

As can be seen in Table 22 each of the banks had developed a simple grading system from which an appraisal rating may be made. The probability assessment was straightforward being either on a scale, for three of the banks, or a % figure for the remaining bank. The impact assessment varied quite considerably with the simplest being Beta bank where a AED figure was allocated; and Alpha bank where a 1 to 5 scale was used within six different scenarios covering financial, media, regulatory, customer, sharcholder and problem management.

The emphasis on estimating a financial impact was summed up in the following comment from one of the managers:

> "We try to encourage people to put a financial impact because I think, especially in banking, that is the only thing that still really gets people interested."

But the problems in doing this were equally recognised:

> "The difficult thing with operational risk is that it's still quite a new discipline in the UAE."

Delta bank saw the output from the risk appraisal process as being an important way of making sure that managers in the Business Units were focusing their priorities in the right areas and avoiding them to concentrate on areas where they may have a particular interest or areas which they understand well and were, therefore, happy to manage. This is an important point and highlights the emphasis that needs to be placed on scaling so that the risks and the Business Units themselves can be judged and compared in relative rather than absolute terms.

In some cases, the role of Internal Audit - independently reviewing and challenging the appraisal ratings that had been established - was identified. Internal Audit would normally leave the area with an agreed audit report, which may necessitate changes to the risk map for that particular Business Unit or area within a Business Unit. This finding is important because it serves to reinforce the role of Internal Audit as the 'Board's guardians' of the ORM framework without direct involvement in the ORM itself.

The analysis of the data in the risk appraisal process, whilst revealing some consistent patterns, also illustrates the importance of controlling the resultant output to ensure that consistent and meaningful conclusions can be drawn from what is an inherently subjective process. This will remain a constant challenge for banks if they are to ensure that they have correctly identified their key risks.

Data: The research found out that the principal source of data used in the risk appraisal process was the experience of those involved in the process (see Table 22).

> "It's just a case of sitting down with the right people and trying to get out of them the knowledge they have in their heads."

Where workshops are used, the risk appraisal would typically have a number of different levels of personnel present to ensure a broad perspective was gained. This would help to remove the appraisal bias:

> "The people who know the nuts and bolts are typically fairly junior but they don't know enough about the big picture to make that kind of assessment, and people that know about the big picture may have lost touch with some of the nuts and bolts."

> "One of the things we have recognised is really making sure we get the right people at the workshops. If you get people who are too low down the management hierarchy then they don't necessarily see the bigger picture of bringing these things together. Yes, we've found we have had to put the groups together quite carefully."

This finding reinforces the subjective and judgemental nature of ORM, vis-à-vis, both identification and appraisal.

A further interesting finding of the study relates to the assessment of current operational risk mitigants as a source of data for appraising an operational risk exposure. Current

mitigants are normally documented at this stage in the risk-mapping process and an overall view is taken on the impact and probability. This is not necessarily the end of the story, however, as other data sources are included (see Table 22) which in aggregate aid the development of a more robust appraisal of the operational risk. The external environment data source and circulars by specialised organisations are interesting examples involving 'keeping an eye on what is going on.' Events of this nature can have important influences on the operational risks faced by a bank and could easily affect the appraisal rating in terms of either impact or probability. Such events can occur in a variety of places, for example, regulatory pronouncements, changes to legislation, technology issues and product developments. External events are recognised as a potential source of operational risk in Basel II and banks must ensure that they figure them prominently in the risk appraisal data.

The output from this part of the process involves summarising the data on the identified risks together with their appraisal ratings thereby producing a total picture of the overall operational riskiness of the Business Unit or area within a Business Unit. These are referred to in different ways by the banks but in essence they equate to the same thing.

4.2.6.1 Main Findings

Analysis of the data revealed that operational risk estimation and evaluation were being done concurrently. The output from each phase had a different emphasis with one focusing on probabilities (estimation) and the other on at least financial impact (evaluation). The risk appraisal process can be split into three phases: responsibility, process and data.

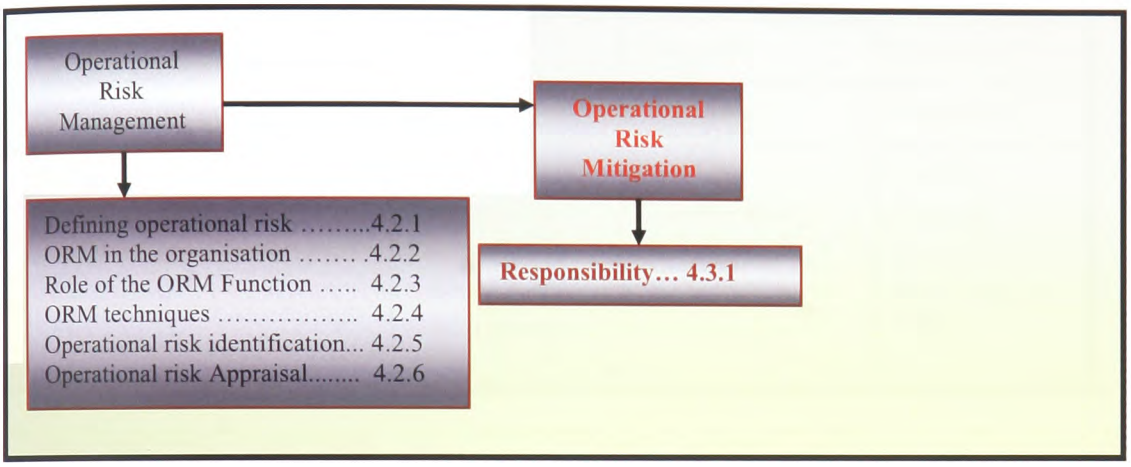
Responsibility: Analysis of the data revealed that the primary responsibility for operational risk appraisal mirrored that of operational risk identification. The managers in the Business Units had the responsibility for appraising operational risk although they might be aided by specialist resources when the situation demands so. Nevertheless, the Corporate Operational Risk Function is more influential in the results that are produced.

Process: In all of the banks the process used to appraise operational risks involved a subjective or judgemental assessment of the probability and impact of the risk, primarily through the workshops, with emphasis on estimating the financial impact.

Data: The research found out that the principal source of data used in the risk appraisal process was the experience of those involved in the process. A further finding of the study relates to the assessment of current operational risk mitigants as a source of data for appraising an operational risk exposure. External environment data source and circulars by specialised organisations were examples involving 'keeping an eye on what was going on.'

4.3 Operational Risk Mitigation

4.3.1 Responsibility for Operational Risk Mitigation



The first set of questions that this research set out to explore were (section1.2.3):

- Who is responsible for operational risk mitigation?
- If more than one functional unit has the responsibility, on what basis is the operational risk exposure assigned to the unit concerned?

There emerged a consistent pattern with previous sections in terms of responsibility for operational risk mitigation, namely, it remains the Managers of the Business Units. This can be seen in Table 23, which shows the results of the data analysis.

Table 23 Operational Risk Mitigation Responsibility: Data Analysis

Mitigation Responsibility	Alpha	Beta	Gamma	Delta
Responsibility	Business Unit	Business Unit	Business Unit	Business Unit
Support	When required	When required	When required	When required
Factors influencing support	Control issue Complexity of risk Option to share risk	Control issue Complexity of risk Cost effectiveness Potential impact Business Unit skills lacking	Control issue Complexity of risk Seeking best practice	Control issue Type of risk Scale of risk Business Unit skills lacking

Source: Analysis of survey data

Comments from the managers interviewed did, however, indicate that the managers of the Business Unit would be supported in their mitigation responsibilities:

"...who can best assess the value of the mitigant?"

"...draw on certain reservoirs of expertise..."

"...use as many people as you can!"

"...there are quite a lot of specialist areas that you can go to..."

Table 23 identifies the factors that would influence the Managers in the Business Unit to seek support. The complexity (type/scale) of the risk and control issues are common elements mentioned in all four of banks. This is not surprising given the range of potential operational risks that exist. For example, the introduction of a control to improve the segregation of duties in a process is a relatively simple exercise to undertake. At the other end of the scale would be the operational risks associated with the introduction of the single

GCC currency, where a number of people would be involved and a project team would probably be set up. As the Business Units are responsible for mitigating the risks, it is the Business Units who would initiate the call for assistance. Such assistance could be from a variety of sources:

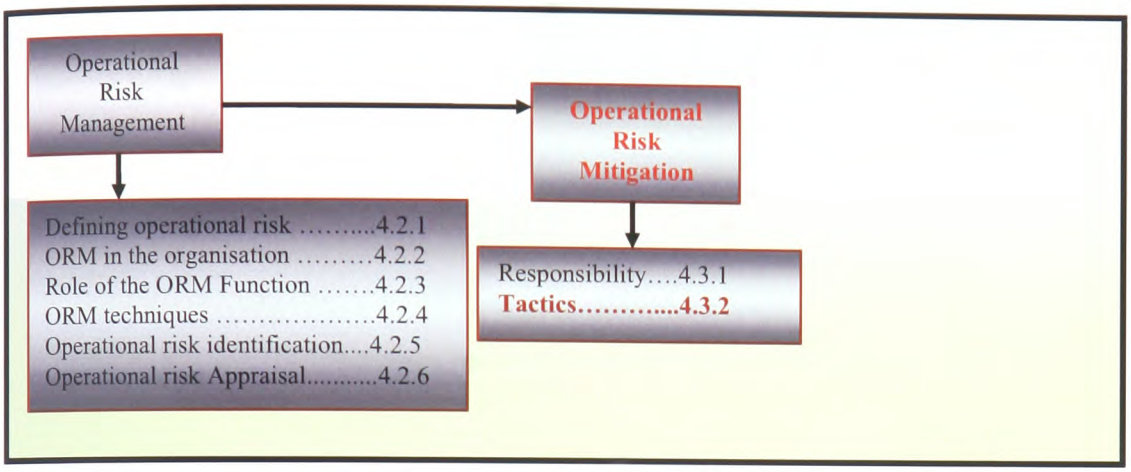
> "Sometimes external consultants can act as the catalyst to get the change (mitigating action) in place"
>
> "Sometimes even just asking from the technology side 'have you got a package that could help?"
>
> "I would certainly encourage managers to approach Risk Managers if they are making major changes to what they are doing in the business in order to discuss some of these implications on their control framework."

Returning to the research questions, the findings suggest that it is the Business Units that have sole responsibility for operational risk mitigation. As a result, the assignments of operational risk to different functions is not carried out, although there is evidence to indicate that the Business Units will seek assistance to mitigate operational risk depending upon the nature and scale of the risk involved.

4.3.1.1 Main Findings

The analysis of the data indicates that there emerged a consistent pattern with previous sections in terms of responsibility for operational risk mitigation, namely, it remains the responsibility of the Business Unit Managers. There are factors that influence the managers in the Business Unit to seek support such as the complexity of the risk and control issues.

4.3.2 Operational Risk Mitigation – Exploring the Tactics Used



The second set of questions that this research set out to explore were (section 1.2.3):

- What tactics are considered before being used to mitigate operational risk exposures?
- How are these tactics established?
- What commonality exists across banks in their risk mitigation tactics, i.e. what may be viewed as core practice?

At this stage in ORM process the managers in the Business Unit should already have identified the operational risks and appraised them by assessing the current mitigants (if any) that are already in place. The dilemma that the managers in the Business Unit face is deciding what, if anything, to do to further reduce the current level (probability/impact) of risks to a level which is more acceptable and tallies with the risk aptitude of the bank.

> "...it's not a case of everything requires additional control. In fact there is a very fine balancing act that is being constantly addressed."

Table 24 shows the results of the data analysis.

Table 24: Operational Risk Mitigation Tactics: Data Analysis

Mitigation – Tactics[65]	Alpha	Beta	Gamma	Delta
Terminate	Yes New product	Yes New product	Yes Leading edge technology Critical supplier	Yes Strategic Temporarily avoid
Treat	Yes Process improve New technology Tightening rules Contingency plans	Yes Process improve New technology Segregation of duties Automating checks Good controls	Yes Process improve Training Procedure guidelines Exception reports	Yes Internal control framework
Take	Yes Outside business Barrier present	Yes Cost/benefit	Yes Cost/benefit	Yes Cost/benefit Potential size
Transfer	Yes Insurance	Yes Insurance	Yes Insurance Internal transfer Outsourcing	Yes Insurance Internal transfer
Other	Sharing		Exploitation	Sharing Relaxation

Source: Analysis of survey data

The mitigation tactics shown equate to those of (Kaple and Gregory 2006), thus:

- Terminate: Avoidance – decide that the risk is too great to follow the course of action.
- Treat: Reduction – decide to reduce the probability and/or impact.
- Take: Assumption – decide to accept the risk and do nothing further.

[65] The reader will note that the tactics all begin with the letter T. One of the managers interviewed introduced the four T's to the author and due to simplicity these words had been used throughout the rest of the text.

- Transfer: Transfer – decide to transfer the risk to a third party.
- Other: Combination – such as risk exploitation and risk relaxation.

Kaple and Gregory (2006) did, however, propose another mitigation strategy, namely 'Hedging', which involves reducing risk through the operation of future markets.

All of the banks use the four T's as mitigation tactics and Table 24 indicates when a particular tactic is used. The following comments are illustrative of some of the scenarios described:

Terminate

> "It would be more of a strategic issue but if you looked at some of our more recent disposals... ... ... some of which you might say would be high in operational risk and, therefore, perhaps there was a factor in that."

> "... there are major impacts across the whole of the operational risk review because if you move to that type of scenario, it actually changes the materiality of a lot of your operations and how they are controlled and mitigated. So, yes there are times when the risk may be so high that the trigger is we actually don't want to do this."

Treat

> "Controls have to be viewed in the wider context of what is it that is absolutely essential to achieve a certain outcome as opposed to that which is nice to have but really perhaps doesn't justify the cost."

> "... can we segregate things better, can we move things into other areas, can we add an automated check, do we need a visual check?"

Take

> "...one of the key risks is systems with a single point of failure...you would look at avoiding risks by having in place some contingency routing mechanism."

> "Let's take for instance, IT security. You're always going to have people who can have access to every part of your system. There is no computer system that has been

built that can remove that risk. Therefore you have to accept that risk to some extent."

Transfer

"...if you can't offset it, you have to guard against financial loss. You may take out some sort of insurance."

"Can I get assistance from anywhere in the business to help with any of that? Part of - I suppose - bundling the risk up, we're not only talking about insuring the risk internally, but are there internal areas of the business who can help me with this? Can I outsource it to another area of the business because they have expertise in that area? That is certainly looked at."

These findings indicate that the tactics that may be used to mitigate an operational risk are in line with those quoted in the literature. The 'Treat' option was the most often quoted (a point also confirmed by the critical incident analysis – see section 4.7) and this finding confirms the view of Basel II that operational risk is practically addressed through a firm's internal control framework.

An interesting issue raised in Delta bank relates to the overall level of controls in a given risk situation compared to the appraisal of the risk.

"Where something is a low priority, and it looks like you are over controlling it, I would like to think the Business Unit will begin to strip out of the unnecessary layers of control, which I think a big organisation like this has built up over history and controls get layered on top of each other without really questioning why they're being done."

The author has referred to this as 'risk relaxation' as the objective is to reduce rather than increase the number of controls (Palfi 2007). This is an important finding as it demonstrates

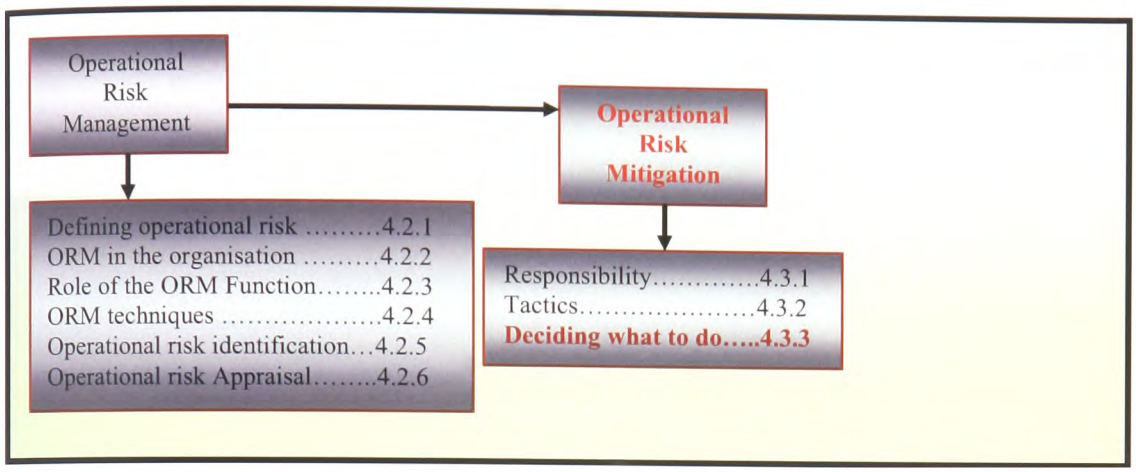
how the operational risk mapping process may be used as a tool to enhance the overall efficiency of the internal control processes in operation.

The final tactic noted by one respondent in Gamma bank was exploitation of the operational risk. The specific example quoted was using leading edge technology where the bank may evaluate that the business benefit outweighs the operational and strategic risks involved. This tactic is the other side of the coin to risk avoidance and illustrates the positive side of risk-taking.

4.3.2.1 Main Findings

The analysis of the data indicates that there are a number of tactics available to all of the banks in mitigating operational risks, although the core tactics may be represented by the four T's (Terminate, Treat, Take and Transfer), with the 'Treat' option being the most commonly used. These tactics have been established as part of the development of the risk-mapping framework and are based on those found in the literature.

4.3.3 Operational Risk Mitigation – Deciding What to Do



The third set of questions that this research set out to explore were (section 1.2.3):

- What is the process used for deciding upon the risk mitigation strategy to adopt?
- What is the process used to ensure that the risk mitigation decisions are adequately communicated and reported?

The focus of the discussions in this area of operational risk mitigation was on who decides the mitigation tactic to employ, what is the process used for selecting and implementing the tactic and what follow-up procedures are used to track the efficiency of the action taken. Consistent with the previous phases of the risk management process, the decision maker was mainly the Business Unit (see Table 25). This situation arises because it would ultimately depend upon a number of factors relating to the risk and the authority of the Manager in the Business Unit:

"...the scale of what is being decided."

"...for significant issues the Risk Management Committee would be involved."

"...within discretionary levels of expenditure."

"...anything which is going to involve a project going into AED 1 million will go up the line."

Table 25: OR Mitigation Selection Procedure and Follow-up

Mitigation: Selection Procedures and follow up	Alpha	Beta	Gamma	Delta
Decision Maker **Escalation Factors**	Mainly Business Unit Scale of risk Cost of action Proposed tactic Approval limits	Mainly Business Unit Scale of risk Cost benefit Level of change Technology impact Customer impact	Mainly Business Unit Scale of risk Cost benefit Resources needed	Mainly Business Unit Scale of risk Cost benefit
Selection process **Factors**	Informal Nature of risk Priorities Amount of work Others involved	Informal Nature of risk Current controls Tracking	Informal Nature of risk Current controls Previous action	Informal Nature of risk Current controls
Follow-up	Informal at Business Unit level	Informal at Business Unit level	Tracking system at Business Unit level with review	Informal through Internal Audit reviews KPIs Personal objectives.

Source: Analysis of survey data

An escalation procedure existed in the banks when the Business Unit could not unilaterally decide on the course of action. This escalation procedure was linked to a number of factors (see Table 25), which appeared to be well understood in the banks. The scale of the risk was a common factor as was cost, i.e. the estimated amount required to mitigate the risk. Where a cost was involved in taking appropriate mitigation action (normally for 'Treat' as per Table 24) then a cost/benefit justification would normally be prepared. This finding is interesting because it illustrates the constraints that managers face in mitigating their

operational risks. These constraints are imposed upon them by the internal environment (policies and rules) of the bank in which they operate and will vary from bank to bank. A tight command control structure will impose different and more sever constraints to a less formal empowerment regime. This issue can be extended further to take into account the manager's own perception of the risk (in terms of what can be done to mitigate the risk down to an acceptable level). Where a tight command control structure exists this perception is of less relevance than in environment regime where managers are able to exercise more personal discretion.

None of the banks had a system of formal procedures for selecting a particular mitigating action (see Table 25). The nature of the operational risk being mitigated combined with the appraisal that has previously been carried out will normally determine by default the mitigation action that needs to be taken. The selection order usually began with an examination of the control environment:

> "In practice, I would say if you took any risk issue the first thing is to look at the level of controls you have around that and if you can improve your internal controls that generally is the most cost effective mechanism."

This finding confirms the comments of Basel II that most operational risks are managed within the internal control environment.

The final phase in the risk mitigation process that emerged from the data analysis was the follow up action that was in place to ensure that the mitigation tactic/action plan was being implemented. There was little consistency across the banks in this area (see Table 25). In two of the banks, the follow up was informal at the Business Unit level. Internal Audit

involvement was mentioned in one bank but this was not 'systematic' and linked to the action plan as part of normal audit procedures. The evidence in Gamma bank indicated that it had a structured approach:

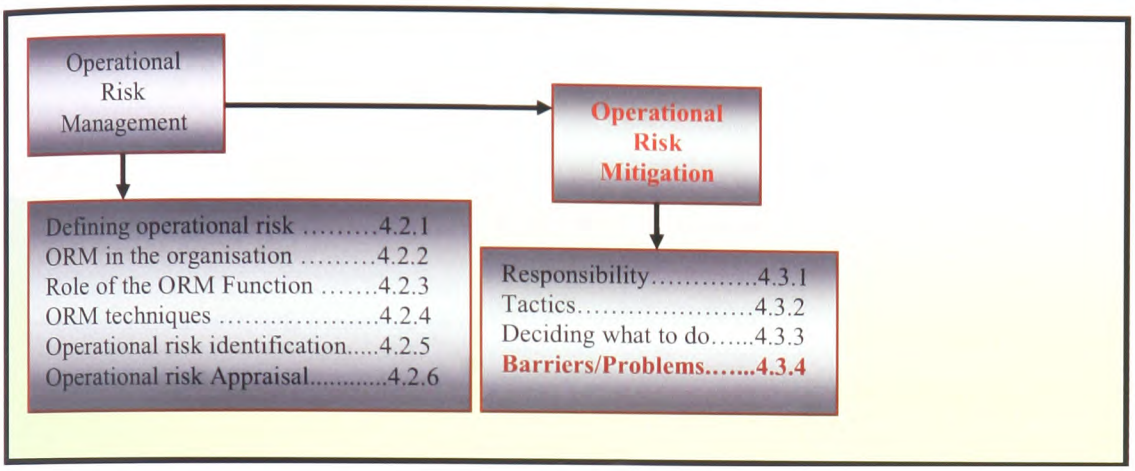
> "...we also have a record of all the action plans in place, besides all the risks, which we keep on our central data base. So that, every quarter currently, we ask for a re-visit exercise, to go back and see what's happening with the action plans, has it been implemented, has it lapsed, is it no longer relevant, etc, to give a status report on how they are going about it."

At the time of the interviews, 86% of the action plans in Gamma bank had been implemented and the controls were in place and the other 14% had not yet been implemented. This finding is important because it suggests that, with the exception of Gamma bank, effective follow-up procedures may not yet be in place to monitor actions to mitigate operational risks, thus leaving the other banks with possible exposures.

4.3.3.1 Main Findings

Analysis of the data indicates that the Business Unit is responsible for deciding the mitigation tactic to deploy. The findings also indicate that the process used in the selection of the appropriate mitigation tactic is informal and based upon the nature of the risk involved. The follow-up process in most banks is not well structured. An escalation procedure existed in the banks when the Business Unit could not unilaterally decide on the course of action due to constraints imposed by the internal environment.

4.3.4 Operational Risk Mitigation – Barriers/Problems Faced by Management



The fourth set of questions that this research set out to explore were (section 1.2.3):

- What are the major barriers to implementing operational risk mitigation actions?

The result of the analysis in this area can be found in Table 26.

Table 26: Operational Risk Mitigation Barriers: Data Analysis

Mitigation – Barriers	Alpha	Beta	Gamma	Delta
Main barriers	Cost and resource Ignorance Reputation Inertia No solution Organisation	Cost Ignorance Reputation Inertia System fragilities Commercial pressures Customer reaction Establish priorities	Cost and resource Ignorance Reputation Change management Timescales Risk appetite	Cost Ignorance Reputation Changing business environment Time
Also noted	Politics	-	-	-
Related matters	-	-	Budget constraints	-

Source: Analysis of survey data

The research found that cost (or more precisely cost versus benefits not being justified) linked to budget constraints (in case of Gamma bank) was a common theme. Additionally,' ignorance' was mentioned as a barrier in all of the banks:

"...lack of risk awareness"

"...lack of understanding of risk in the particular environment"

"...ignorance of how particular risk mitigation techniques may be implemented"

Reputation was also identified to be a barrier in all banks. This is due to the fact that culturally speaking; the UAE commercial banks are owned by wealthy people who would not want to be exposed to a deteriorating reputational profile:

"...it is a reputational issue..."

"...it is not in favour of the owners' reputation."

Table 26 illustrates the other barriers that were identified by managers. The fact that there are a number of barriers is probably indicative of the broad nature of operational risk. From a mitigation point of view, this suggests that operational risk can be adversely influenced by a whole range of factors. The risk appetite mentioned at Gamma bank was particularly interesting:

> "I think something interesting in the corporate arena is that the actual appetite for risk is not clear in some cases. It may be clear to the strategic thinkers at the centre, and they may have a good idea, but it's not that helpful to the practitioners if they are not aware what the appetite is for accepting operational risk."

4.3.4.1 Main Findings

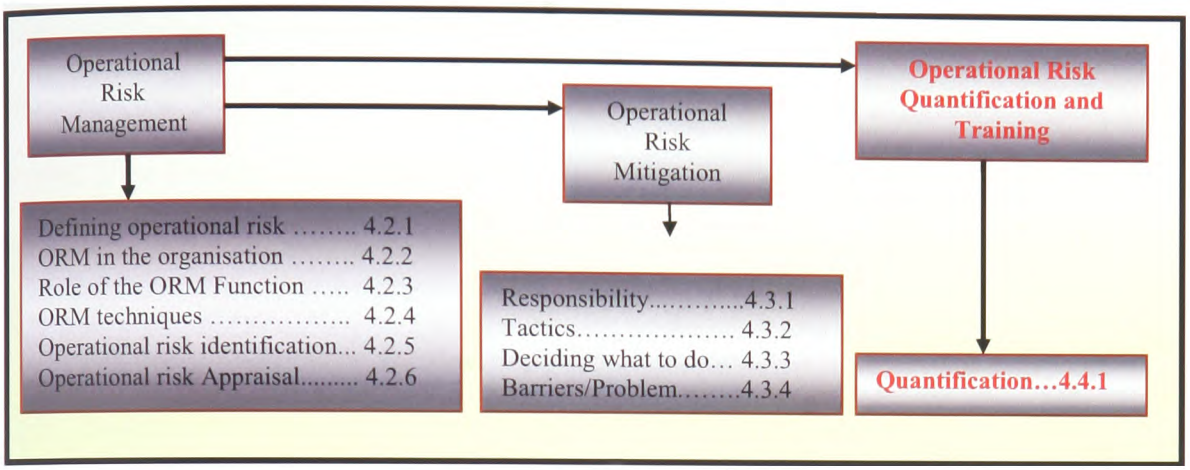
The analysis of the data indicates that cost linked to budget constraints is a common barrier, besides resource, ignorance and reputation.

The findings are important because they identify the types of problems that managers face in mitigating operational risk. The decision as to how to mitigate a particular operational risk will have to take due consideration of the barriers or constraints that exist within the organisation. Business Units will have different needs in terms of risk mitigation based upon their inherent risk profile. There is no 'one size fits all' way to mitigate operational risk and the interplay of the various 'actors and factors' involved is an area where further developments will be required if the organisation is to 'guarantee' its level of residual risk.

4.4 Operational Risk – Quantification and Training

This section discusses the findings in two areas important to ORM: quantification and training. Quantification has received a lot of attention in the practitioner's literature as a result of banking regulatory requirements, which require capital to be put aside to cover potential operational risk losses (discussed in section 2.3.4.7). Training was identified as an important area that needs to be thoroughly covered, and can be an area for further research.

4.4.1 Quantification



The results of data analysis for quantification can be seen in Table 27. All of the banks had a formal methodology for calculating their total operational risk exposure as per Basel II recommendation, and there was general recognition that there was still a lot to do in this area. The plan is to 'improve as you move' on a continuum from the BIA, through the TSA and ultimately to the AMA within 3 – 5 years. Again, this is in line with Basel II recommendations and the CBUAE mandate (see section 2.4.2.1).

Table 27: Operational Risk Quantification: Data Analysis

Quantification	Alpha	Beta	Gamma	Delta
Methodology	Done : BIA	Done : BIA	Done : BIA	Done : BIA
Time frame for AMA	3 – 5 years	3 – 5 years	3 – 5 years	3 – 5 years
Level of support	Skeptical about value of results	Worth doing, but still a lot to do.	Supported	Mixed, depends on the risk

Source: Analysis of survey data

Support for quantifying operational risk was 'mixed' with a majority of the managers interviewed believing it would not help them in their day-to-day management of operational risk. Nevertheless, it is a regulatory requirement by the CBUAE. Those who worked in the Corporate Risk Function, who would probably be responsible for carrying out the work, were generally more inclined to accept quantification as something that had to be done:

> "At the end of the day, it will make operational risk decisions much easier. At the moment, there is far too much analysis, and thought processes having to go around a decision and not enough hard evidence that we can actually sit back and say 'let's make this decision based on the right criteria."

> "I think it is possible for financial organisations to value operational risk by following what Basel II came up with about quantification and then trying to impose something from top down to quantify operational risk. That is certainly what we do using financial methods but I don't think it is an accurate reflection of what the risks are within the bank."

For the other managers and particularly those who operated at the 'sharp end' there were generally adverse comments towards the idea and in some cases contradictory points of view:

> "I am sure there are means of devising measures of it, but you have got to bear in mind that any measures might be used in order to take business decisions and if measures are inaccurate you get inaccurate decisions, and I think there is a huge risk of that happening."

> "I think you may have greater control over operational risk if you actually put aside the hurdle of quantification and simply recognise these are major risks the banks can be running with a certain amount or resource has to be put into controlling them."

> "Spending a great deal of time and money on coming up with a number is not necessarily going to get any institution to concentrate on improving its controls."

> "...with some operational risks, my personal view is that you are better not doing it at all because it might be quite misleading."

One manager offered some advice to the regulators:

> "If I were a regulator, I would be looking for distinct evidence that there was a decent operational risk management framework in place. That there was a decent amount of risk awareness in place in the organisation where the risks are likely to occur and that any quantification was built from a view that the organisation had of their potential vulnerability of those risks occurring."

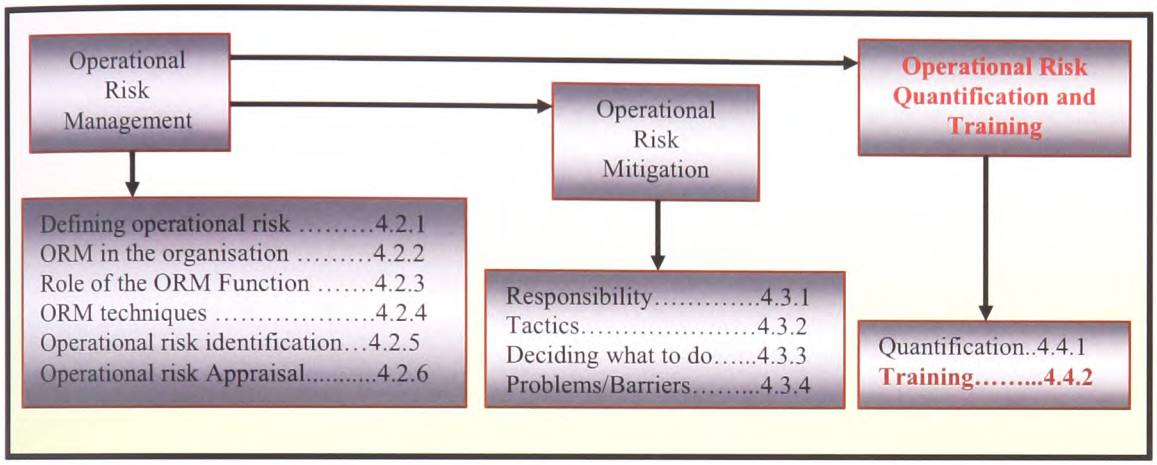
These findings are particularly significant as they confirm the view that some banks are not well positioned in relation to developing a methodology for quantifying operational risk using the advanced methods (TSA and AMA) but more importantly, they reflect the views of others who have written on this subject (Ong 1998) that operational risk is more of a management issue and less a quantification issue. This may imply that operational risk prevention (management) and measurement (quantification) should be seen as mutually exclusive since a financial loss will result from inadequate management control rather than a lack of measurement techniques.

4.4.1.1 Main Findings

The results of the data analysis (see also section 4.2.3.1) indicate that the responsibility of operational risk quantification rests with the Corporate Operational Risk Function. The results of data analysis for quantification also indicate that all of the banks have a formal methodology for calculating their total operational risk exposure as per Basel II recommendation using the BIA, and there is general recognition that there is still a lot to do in this area, with the intention to move on a continuum from the BIA, through the TSA and

ultimately to the AMA within 3 – 5 years. Again, this is in line with Basel II recommendations.

4.4.2 Training



The results of the data analysis for training can be seen in Table 28. The research found that there is no consistency across the banks in terms of their approach to operational risk training. Alpha bank had developed a formal operational risk awareness training course consisting of two modules for both staff and management. At the other end of the scale, Delta bank had not yet considered training, reflecting the pilot stage of their operational risk framework development.

Table 28: Operational Risk Training: Data Analysis

Training	Alpha	Beta	Gamma	Delta
Approach	Formal	Informal	Informal	None
Method	Risk- mapping Framework	Risk- mapping Framework	Risk- mapping Framework	None
Focus	Management and staff	Management	Management	None

Source: Analysis of survey data

There were many comments in support of training:

> "...training needs to be focused more on the meaning of 'managing operational risk' and particularly around people's personal responsibilities."

> "...educating staff to understand what controls are and where they are required."

> "I think the Bank could benefit from some sort of coordinated risk training."

> "...enabling within the organisation at every level an appreciation of the consequences of actions or inactions."

In three of the banks the risk-mapping framework was seen as an 'informal' or indirect training tool for the managers in the Business Unit. Comments from managers who worked in the Business Units indicated that training was seen as an important area:

> "We are moving towards getting them (staff in the Business Unit) to think risk. We've acquired some operational risk training packages ... ... in the sense of ticking: here are your key control processes and here are your risk processes."

But there were other factors that needed to be considered in raising the awareness of operational risk:

> "Whatever risk-mapping process you put in place, if you don't have enough experienced people around in the business long enough to understand where the risk is, and if you have a lot of turnover, and if you are not training your people right, you introduce risk and the soft factors are quite important in looking at that: training, development and retention of staff."

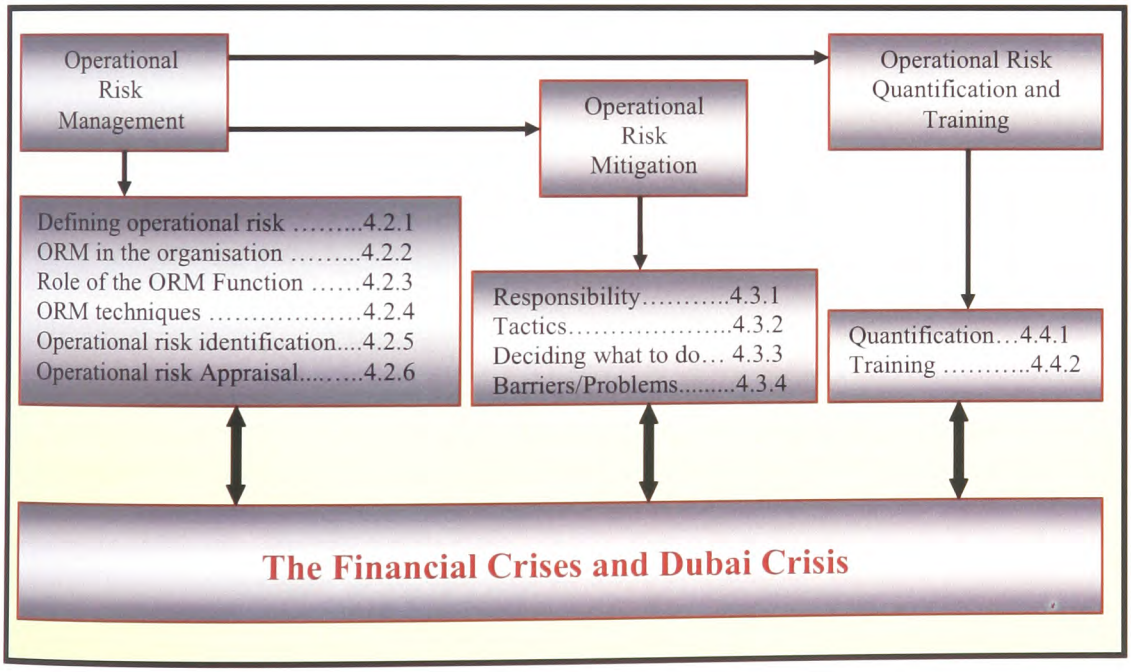
The findings are particularly important in the context of the problems that managers face in managing, and, therefore, mitigating operational risk. Ignorance (see Table 26) was cited by all of the banks as being an important barrier to effective operational risk mitigation and

it could be argued that the best way to overcome this is through an effective training programme.

4.4.2.1 Main Findings

The results of the data analysis for training reveal that there is no consistency across the banks in terms of their approach to operational risk training. Most of the banks see the risk-mapping framework as an informal or indirect training tool. Comments from managers who worked in the Business Units indicated that training was seen as an important area.

4.5 Operational Risk and the Financial Crisis and Dubai Crisis



This section discusses the findings in relation to operational risk and the Financial Crisis and Dubai Crisis (Financial Crises) discussed in section 2.4.1. This topic has received a lot

of attention in the literature as a result of the consequences of the Financial Crises and the banking regulatory requirements (FSF 2008, Lilco 2008, Elliott 2008, Saif and Choucair 2009). The detailed causes of the Financial Crises are outside the scope of this study, however, the operational risk that contributed to these Financial Crises in the context of the UAE commercial banking will be discussed in more detail.

Due to their descriptive nature, the results will not be presented in a tabular form. The aggregate feedback analysis will be presented after each area discussed with the interviewees without reference to a specific bank. Some important quotes will also be presented, and will be followed by analysis of the feedback. The following are the areas discussed with the interviewees and the related feedback:

Financial Crises Predictability and Recurrence Prevention Measures:

> "...the Financial Crises were predictable since the economy became too dependent on financial services leading to a credit crisis with severe implications..."
>
> "The UAE banks were extending loans to finance property purchases at exaggerated pricing."
>
> "Severe decrease of property price in Dubai was due to increased supply and reduced demand due to lack of purchasing power or liquidity caused by the Financial Crisis."

The above quotes shed light on the issues that prompted the Financial Crises. The data analysis indicates that the Financial Crises were predictable since financial institutes, including the UAE commercial banks, were extending loans to finance property and other purchases at extremely high or bubble pricing. Hence, the economy became too dependent on financial services without due consideration to the instigated risks.

> "The UAE banks need to develop cutting-edge risk management structures across credit risk, market risk and integrated ORM to stay ahead of the competition, counteract crises and ensure they are on top of new regulations..."

Another issue that has been pointed out is that the UAE commercial banks need cutting-edge or robust risk management structures and integrated ORM frameworks in order to counteract Financial Crises, stay ahead of competition and ensure they are on top of new regulations. They need to ensure that the ORM identifies the drivers of the operational risk events and measures their impact across the banks over time. This could be done using predictive models based on macroeconomic conditions, market and credit risk data, and key risk indicators; supplemented by stress testing, business environment monitoring and internal control factors. Thus, the vulnerabilities or gradual build up of imbalances related to funding mismatches can be identified.

> "It boils down to ensuring the right risk aware culture... ...this is a Board responsibility..."

One more important point that the data analysis revealed is that an operational risk aware culture must be integrated into the culture of the bank, and this will need to include mandate, leadership and commitment from the Board. The Board must translate risk strategy into operational objectives, and assign risk management responsibilities throughout the organisation. It should support accountability, performance measurement and reward, thus promoting operational efficiency at all levels.

> "Operational risk management and the business need to work hand in hand to create what you can call risk aware culture..."

Another issue highlighted is the need for ORM and Businesses to work together to create a more conscious risk culture within the bank.

> "...healthy corporate governance is the driver..."
>
> "...what is needed is a more prudent and transparent regulatory regime that encourages better ORM..."

To conclude, the Financial Crises were predictable, and there is obviously a great need to focus more attention on cutting-edge or robust risk management structures, healthy corporate governance, risk aware culture in the banks and more effective regulation in order to avoid recurrence of such Financial Crises.

The Operational Risks that Contributed to the Financial Crises:

> "...too much liquidity leads to too much credit...what about the operational risks behind that? Can the current setup cope..?"

This quote captures the operational risks behind the Financial Crises. The data analysis indicates that the operational risks that contributed to the Financial Crises included allowing large credit growth nourished by a long period of low interest rates and abundant liquidity which increased the amount of operational risk that borrowers and investors took. The increase in credit growth outpaced ORM capacity to manage the associated risks, which is an operational risk in itself.

> "... banks are reactive to operational risk management. We need is to be truly proactive..."

One more important point that the data analysis revealed is related to adopting reactive rather than proactive strategies of operational risk monitoring and detection, thus, the business model for banking moved towards an equity culture with a focus on faster share price growth and earnings expansion, which lead the banks to focus mainly on the expected return side of their investment leaving the operational risks to manifest themselves.

> "...the biggest failures of risk management are due to weak risk governance structure, weak vision of risks and lack of a well defined capital allocation strategy..."

The significant bank failures are mainly due to inappropriate risk governance structure, disaggregated vision of risks and lack of a defined capital allocation strategy. Most banks used to grow their lending portfolios at bubble conditions driven by market demand without a clear capital allocation strategy. A capital allocation strategy should be thoroughly defined for the short and long term using a risk appetite framework to specify the bank's risk capacity (maximum risk tolerance) and risk appetite (desired risk tolerance).

> "...Ultimately, more regulation is crucial. However, we have to guarantee it is going to function well."
>
> "...what is needed is a more practical and transparent regulatory system that encourages better ORM..."

Finally, a 'weak' regulatory framework based on the belief that banks could be trusted to regulate themselves is among the operational risk sources of the Crises.

To conclude, the operational risk that contributed to the Financial Crises included extending excessive credit without addressing the operational risks instigated, weak operational risk governance structures, adopting reactive rather than proactive ORM strategies, disaggregated vision of risks, lack of a well defined capital allocation strategy and week regulatory frameworks.

The Impact of the Financial Crises on the UAE Commercial Banks:

> "...borrowers could no longer pay..., you can call it bad debts..."
>
> "You need more liquidity to keep the momentum, customers have expectations...you do all you can to maintain customer faith..., it is all about customers..."

The data analysis indicates that as a result of the Financial Crises, the UAE commercial banks suffered many consequences, such as bad debt accumulation, lack of liquidity for lending, loss in asset value, loss of faith in the banking system by the general populace and withdrawal of foreign depositors' money resulting in more liquidity shortage.

Mitigation of the Operational Risks that Contributed to the Financial Crises:

> "...yes, the UAE Government intervention was very timely..."

The data analysis indicates that the Government of the UAE supplied liquidity to all National banks, guaranteed depositors' money and guaranteed interbank loans. This intervention by the CBUAE has arrested the panic, effectively stabilised the UAE financial system, and helped restore depositors' confidence. On the other hand, there was no evidence that the banks themselves took any measures to mitigate the operational risks that contributed to the Financial Crises. This is an important point since it reveals that the UAE

commercial banks were too dependent on the UAE Government measures, leaving their ORM systems to evolve at the normal pace. The author would contend that this is an operational risk in itself that needs to be addressed in order to be prepared for future Financial Crises, should they occur.

Stress Testing in the UAE Commercial Banks:

> "We are looking positively at stress testing, after all this is a measure to help us to put things right..."

The data analysis reveals that stress testing has not yet been conducted in the UAE commercial banks. However, it has been mandated by the CBUAE and is planned to commence within the next year in all commercial banks.

Some Managers gave optimistic and comforting comments:

> "The UAE banks are not too global; hence, they did not suffer so much from the Financial Crises."
>
> "Capital adequacy in the UAE banks is more than BCBS requirements. This is a reputation issue..."
>
> "Cost of capital in the UAE banks is very low because many people do not take interest due to Islamic reasons, resulting in high profit margin."

The three comments are of particular interest sense they are indicative of some comfort as to the lesser extent the UAE banks were affected by the Financial Crises. Nevertheless, the author would argue that the intervention of the CBUAE to mitigate the risk by pumping sufficient liquidity in the UAE commercial banks was the main comforting issue when it came to restoring confidence in the UAE banking sector.

The research findings above indicate that the fallout from the Financial Crises has illustrated that many sources of risk were triggered or at least propagated by vulnerabilities in ORM, which has not kept pace with financial innovation. At the same time the study revealed that the UAE banks are at immature stages of ORM development and show considerable dispersion in ORM practices while falling short of integrating operational risk as a vital process.

Worldwide, the scale of the Financial Crisis has revealed major shortcomings in ORM, and triggered an avalanche of reforms in response to the apparent failure of the existing regulatory framework.

Against the background of new sources of threats to financial stability, operational risk is becoming a salient feature of risk management in the banking industry. Amid the turbulence of the Financial Crisis, operational risk has become well recognised in the banking industry. The increase in scope of operational risk is largely explained by noting that operational risk amplifies system wide risk levels and has a greater potential to manifest itself in more harmful ways than many other sources of risk, given the increased size, interconnectedness, and complexity of banking industry.

The findings are particularly important in the context of the ORM shortcoming in the UAE commercial banks and what needs to be done to mitigate these shortcomings in order to prevent the recurrence of such Financial Crises.

To conclude, the analysis of the findings indicates that the UAE commercial banks need to enhance ORM in order to counteract Financial Crises, stay ahead of competition and ensure being on top of new regulations. The author would argue that the way forward to achieving a sustainable level of excellence in this regard, is by adopting an integrated ORM framework. This topic will be discussed in detail in the next Chapter where the drivers for a proposed integrated framework are addressed (section 5.2.4).

4.6 Case Summaries: Common Themes and Differences

The cross-data analysis identified a number of emerging themes and important differences between the banks. This section discusses the results of the analysis in this respect.

4.6.1 Common Themes

The following themes appear to be the most common across the banks:

1. All four banks were negatively impacted by the Financial Crisis and Dubai Crisis.
2. The definitions of operational risk used by the banks were either (two cases) identical to Basel II or (two cases) adapted Basel II. All the managers interviewed were aware of the definition and had a good understanding of it.
3. All four banks have recently deployed a form of operational risk software application. However, none of the banks is utilising the application to the maximum efficiency. The application in all banks is used mainly for data storage and retrieval. Training on the use of the application is on-going in all banks.

4. All the Corporate Operational Risk units within the four banks reported to the Corporate Risk Function and had a good working relationship with Internal Audit.
5. All four banks used a tailored risk-mapping framework to manage operational risk, although Delta bank was piloting its use in two Business Units at the time the study was undertaken.
6. All banks had some form of key risk indicators to monitor operational risk exposures.
7. Responsibility for ORM (all phases) was found to be with the managers in the Business Units. The broad nature of operational risk meant that they could be helped by specialists when the need arose. The factors that would influence them to seek assistance with mitigating an operational risk were various, but revolved around the complexity of the risk and the control issues involved.
8. The processes involved in ORM were subjective and judgemental and relied heavily on the skills and experience of the people involved in the process in all four banks.
9. The core tactics used to mitigate operational risk appeared to be similar in all four banks. The most commonly used tactic emerging from the study is reducing the risk (probability and/or impact) by improving the internal control framework.
10. All banks recognised a number of barriers or constraints in mitigating operational risk. The two which appeared to be the most important for the banks were (1) cost, in the context of cost versus benefit; and (2) ignorance, meaning the lack of risk awareness of the 'Management and Staff.'

Considering the fact that there is a central body (CBUAE) providing guidance and a common approach on how to manage operational risk, it is hardly surprising to find that the frameworks for ORM are so similar. Indeed, all of the banks' operational risk frameworks are aimed at managing rather than measuring operational risk. The four banks involved in this study have been focusing their attention on implementing a framework to solve the problem of explicitly managing operational risk rather than actively pursuing a measurement strategy which should, in theory, help them to achieve better capital allocation.

4.6.2 Major Differences between the Banks

Despite some commonalities in approach, there were nonetheless some important differences. These have been summarised in Table 29.

Table 29: Major Differences between the Banks

Area	Alpha	Beta	Gamma	Delta
Operational risk definition Exclusions	Market, credit	Market, credit	Market, credit, strategic, reputational	Market, credit, strategic reputational
Organisation Use of Business Unit in ORM Other OR risk roles Operational Risk Committee	Developing None No	Developing None Part of risk committee	Well developed Part-time risk officers Yes, several	Early days None Yes, one
Role of Corporate Function Mitigating OR's which span BU's OR Unit works with BU ORM OR Unit works with Business Unit	Coordinate effort Often Often	Coordinate effort Often Occasionally	No Very often Occasionally	No Developing Developing
ORM techniques Extent of coverage	50% complete	One cycle done	One cycle done	Pilot stage
OR identification and appraisal Process Impact focus	Mainly formal plus informal AED: 1 – 5 scale using different scenarios	Mainly formal plus informal AED: Figure	Mainly formal AED: 1 – 6 scale Risk > AED 1 m: 1 – 4 scale	Mainly formal AED: 1 – 6 scale AED: number ranges + consequential impact
OR mitigation Other tactics Follow-up Barriers	Sharing Informal at Business at Unit level Various, mainly specific to the bank	- Informal at Business Unit level Various, mainly specific to the bank	Exploitation Tracking system at Business Unit level with review Various, mainly specific to the bank	Sharing, relaxation Informal through IA reviews, KPIs and personal objectives Various, mainly specific to the bank
Training Approach Methods Focus	Formal Framework Management and staff	Informal Framework Management	Informal Framework Management	None None None

Source: Developed by the author

The differences tend to be variations on a theme rather than specific differences in approach, for example, the impact assessment of an operational risk used different scales to measure the financial impact. In some cases it appears that a bank has developed a particular area to a high degree of resilience. For example, the tracking system in Gamma bank seemed to be very robust and offered a high degree of certainty that the agreed mitigation would be implemented.

A discussion of the data analysis was presented in this section highlighting the common themes and major differences between the four banks.

4.7 Critical Incidents and Triangulation

As discussed in section 3.3.3, Triangulation has been employed in this study using *Critical Incident Techniques* (CIT's) to validate the results (Serenko 2006), since CIT's provide data that can be used to either substantiate or reject the data analysis findings. The approach is consistent with the fourth type of triangulation as identified by Stake (2005).The author has selected four from those listed to illustrate the problems that managers face in dealing with operational risk incidents (Note: The incident number refers to *Appendix C*). The table after each incident depicts further critical incident data analysis results compared to the study findings. The figure on the left side corresponds to the sub-suction in this Chapter where that area of ORM was analysed based on the study data.

Incident No. 5 – File of Transactions Transferred

According to Basel II classification (Basel II, p. 257), this critical incident is an example of the seventh source of operational risk (see section 2.3.4.2): Execution, Delivery and Process Management - data entry errors, accounting errors, failed mandatory reporting and negligent loss of client assets.

A file of outstanding transactions was transferred from one Business Unit to another (following an acquisition by the bank). The Business Unit in charge discovered that the

record keeping of the original Business Unit was unsatisfactory, and as a result, errors in the transactions were appearing. This situation is still ongoing and the challenge for the bank, now that the risk had been identified, is to assess whether the amount of work involved in totally mitigating the risk is cost effective and worth the effort involved. As the manager put it:

> "We're weighing up at the moment whether the risk warrants the effort to go back in and review every one of those thousands of transactions and go on through them all again in detail and highlight whether any of them has been improperly filed. That is an issue on my desk today. I have asked how many transactions there are. How long would it take to do it? Or, do we accept that we should have some reserve for occasional losses which might occur?"

This comment reflects the need to put some form of measure on the risk before deciding how to mitigate it. The two possible tactics being considered by the Business Unit are 'Take' – accept there are errors and live with them – and 'Treat' – check all the deals and remove those that have been improperly filed.

This incident supports the data analysis findings mainly concerning the need to assess the scale of the risk and the remedial cost before deciding the appropriate course of action.

Table 30: Critical Incident No. (5) Data Analysis vs. Study Data Analysis

Operational Risk Management Area		Conformance to the Data Analysis
4.2	**Operational Risk Management**	
4.2.1	**Defining Operational Risk** • The operational risk in this incident is included in the definition of operational risk.	Y
4.2.2	**Operational Risk Management in the Organisation** • Operational Risk Managers operate in the Business Units.	Y
4.2.3	**The Role of the Operational Risk Management Function** • The Corporate Operational Risk Function was not involved in	Y

	this incident since the core responsibilities of the Corporate Operational Risk Function are: policy setting, aggregation of operational risk profile, high level reporting, assurance, framework setting, operational risk measurement and loss data maintenance.	
4.2.4	**Operational Risk Management Techniques** • The banks use an ORM framework.	Y
4.2.5	**Operational Risk Identification** • The responsibility for operational risk identification rests with the people who manage the processes and systems. • The main data sources to identify operational risks are the skill and experience of the people involved in the identification process. • Operational risks identification and appraising are done simultaneously. • Frequent monitoring of both potential operational risk sources to assess existing operational risks. • The Audit Function was not involved in this incident since the Audit Function may provide valuable input to those responsible for ORM, but does not have direct ORM responsibilities.	Y
4.2.6	**Operational Risk Appraisal** • Operational risk estimation and evaluation are done concurrently. • The output from each phase has a different emphasis with one focusing on probabilities (estimation) and the other on at least financial impact (evaluation). • The responsibility for operational risk appraisal rests with the Managers in the Business Units. • The operational risk appraisal process is subjective or judgemental assessment of the probability and impact of the risk. • The main data source to appraise operational risks is the experience of the people involved in the process.	Y
4.3	**Operational Risk Mitigation**	
4.3.1	**Responsibility for Operational Risk Mitigation** • The responsibility for operational risk mitigation rests with the Managers in the Business Units.	Y
4.3.2	**Operational Risk Mitigation – Exploring the Tactics Used** • The main operational risk mitigation tactics used are: 'Terminate', 'Treat', 'Take' and 'Transfer'.	Y
4.3.3	**Operational Risk Mitigation – Deciding What to Do** • The Managers in Business Units are responsible for deciding the mitigation tactic to deploy. • The process used in the selection of the appropriate mitigation tactic is informal and based upon the nature of the risk involved.	Y
4.3.4	**Operational Risk Mitigation – Barriers Faced by Management** • The main operational risk mitigation barriers are cost, resource, ignorance, customer reaction and reputation.	Y
4.4	**Operational Risk – Quantification and Training**	
4.4.1	**Quantification**	N

	• The responsibility for operational risk quantification rests with the Corporate Operational Risk Function.	
4.4.2	**Training** • Training was seen as an important tool in all ORM phases.	Y

Key: Y = Yes, the critical incident tallies with the data analysis results of the study.
N = No, the critical incident data does not tally with the data analysis of the study.

Source: Developed by the author

Incident No. 9 – Uncleared Cheques

According to Basel II classification (Basel II, p. 257), this critical incident is an example of the second source of operational risk (see section 2.3.4.2): External Fraud- theft of information, hacking damage, third-party theft and forgery.

This type of fraud was few years ago understood to be quite common in commercial banks and involved customers attempting to draw on cheques, which had not yet been cleared. As such, it is a well-known risk, which always existed:

> "It was always a part of our training, part of our processes to check. Historically we'd known what the losses were, but they'd been accepted by management."

The last sentence indicates that the mitigation tactic used for this risk was 'Take', i.e. to accept the risk. What happened in this particular case was that the amount of losses started to rise significantly, i.e. the impact moved up. As a result, additional technical connectivity (virtual private networks) and procedures were introduced by the Business Unit in an attempt to reduce both the probability and impact. This was, however, seen only as a short-term measure whilst a full-scale change management technological project was instigated to resolve the problem. This latter course of action becomes necessary in banks when any

changes to systems and procedures could potentially have an impact on customers. In the meantime losses continued to escalate, i.e. the mitigation tactic was not working effectively and fraudsters were finding new ways to beat the system. A further procedure was introduced which curtailed the fraudulent activity and reduced losses to an 'acceptable level'. The end solution to the problem, however, involved the change management project team developing technical intranet verification changes that the ineffective procedures could be removed.

This is an example of 'Treat' being used to iteratively mitigate an operational risk exposure. Crucially, the incident illustrates the importance of having follow-up procedures once the risk mitigation decision has been taken in order to ensure that the tactic is working. Another important aspect of this incident is the recognition that there will always be some residual risk (acceptable loss) which will be accepted by the Business Unit, since removing the risk, by including, rigorous control procedures, could have a negative impact upon customer relations.

This incident supports the data analysis findings mainly concerning the constraints (cost and customer reaction) imposed upon the managers when mitigating an operational risk as well as the findings related to the need to ensure adequate follow-up measures are in place.

Table 31: Critical Incident No. (9) Data Analysis vs. Study Data Analysis

Operational Risk Management Area		Conformance to the Data Analysis
4.2	Operational Risk Management	
4.2.1	Defining Operational Risk	Y

	• The operational risk in this incident is included in the definition of operational risk.	
4.2.2	**Operational Risk Management in the Organisation** • Operational Risk Managers operate in the Business Units.	Y
4.2.3	**The Role of the Operational Risk Management Function** • The Corporate Operational Risk Function was not involved in this incident since the core responsibilities of the Corporate Operational Risk Function are: policy setting, aggregation of operational risk profile, high level reporting, assurance, framework setting, operational risk measurement and loss data maintenance.	Y
4.2.4	**Operational Risk Management Techniques** • The banks use an ORM framework. • The ORM framework is based on the 'bottom up' approach. • The banks use incident loss data in order to be more proactive in taking action before an operational risk manifests itself.	Y
4.2.5	**Operational Risk Identification** • The responsibility for operational risk identification rests with the people who manage the processes and systems. • The main data sources to identify operational risks are the skill and experience of the people involved in the identification process. • Operational risks identification and appraising are done simultaneously. • Frequent monitoring of both potential operational risk sources and key risk indicators to assess existing operational risks. • The Audit Function was not involved in this incident since the Audit Function may provide valuable input to those responsible for ORM, but does not have direct ORM responsibilities.	Y
4.2.6	**Operational Risk Appraisal** • Operational risk estimation and evaluation are done concurrently. • The output from each phase has a different emphasis with one focusing on probabilities (estimation) and the other on at least financial impact (evaluation). • The responsibility for operational risk appraisal rests with the Managers in the Business Units. • The operational risk appraisal process is subjective or judgemental assessment of the probability and impact of the risk. • The main data source to appraise operational risks is the experience of the people involved in the process.	Y
4.3	**Operational Risk Mitigation**	
4.3.1	**Responsibility for Operational Risk Mitigation** • The responsibility for operational risk mitigation rests with the Managers in the Business Units.	Y
4.3.2	**Operational Risk Mitigation – Exploring the Tactics Used** • The main operational risk mitigation tactics used are: 'Terminate', 'Treat', 'Take' and 'Transfer'.	Y

4.3.3	**Operational Risk Mitigation – Deciding What to Do** • The Managers in Business Units are responsible for deciding the mitigation tactic to deploy. • The process used in the selection of the appropriate mitigation tactic is informal and based upon the nature of the risk involved. • Adequate follow-up measures should be in place.	Y
4.3.4	**Operational Risk Mitigation – Barriers Faced by Management** • The main operational risk mitigation barriers are cost, resource, ignorance, customer reaction and reputation.	Y
4.4	**Operational Risk – Quantification and Training**	
4.4.1	**Quantification** • The responsibility for operational risk quantification rests with the Corporate Operational Risk Function.	N
4.4.2	**Training** • Training was seen as an important tool in all ORM phases.	Y

Key: Y = Yes, the critical incident tallies with the data analysis results of the study.
N = No, the critical incident data does not tally with the data analysis of the study.

Source: Developed by the author

Incident No. 11 – Incorrect Payment Remittance

According to Basel II classification (Basel II, p. 257), this critical incident is an example of the seventh source of operational risk (see section 2.3.4.2): Execution, Delivery and Process Management –data entry errors, accounting errors, failed mandatory reporting and negligent loss of client assets.

The bank involved has a procedure in place to check the remittance on international payments. This was a double-check procedure before the remittance is made. Despite having a control in place to mitigate this risk, on one particular occasion it did not work and a large payment (several hundreds of thousands of AED) was mistakenly sent to the wrong party. When the incident came to light some of the dues were recovered (but not all) and compensation had to be paid to the correct party. This risk had been identified but it

was considered that there were adequate controls in place for mitigation; and that it, therefore, represented a low probability event. Within the same Business Unit, another operational risk had also been identified relating to staff training/communication in this section, which was recognised as being weak and in need of improvement. A training/communication plan had been developed to mitigate the risk and was due for implementation a few months after the date of the incident. The training/communication risk had, therefore, been accepted for a short period and the mitigation action had been postponed. It was this latter risk which manifested itself in the remittance procedure not being undertaken correctly, thus causing the incorrect remittance to be made.

This is an interesting example of how one risk can cause another one to occur, despite the fact that adequate mitigating actions were in place for both of them. It also highlights the behavioural side of operational risk, a particularly difficult area to manage and quantify. The tactic being used to mitigate these risks was 'Treat' although, as has been noted, the second risk had been 'Taken' for a short period of time. The subsequent decision taken has been to bring forward the implementation of the training/communication plan.

This incident supports the data analysis findings concerning the constraints imposed upon the managers when mitigating an operational risk and also illustrates the cross-linkages between operational risks themselves.

Table 32: Critical Incident No. (11) Data Analysis vs. Study Data Analysis

	Operational Risk Management Area	Conformance to the Data Analysis
4.2	**Operational Risk Management**	
4.2.1	**Defining Operational Risk** • The operational risk in this incident is included in the definition of operational risk.	Y
4.2.2	**Operational Risk Management in the Organisation** • Operational Risk Managers operate in the Business Units.	Y
4.2.3	**The Role of the Operational Risk Management Function** • The Corporate Operational Risk Function was not involved in this incident since the core responsibilities of the Corporate Operational Risk Function are: policy setting, aggregation of operational risk profile, high level reporting, assurance, framework setting, operational risk measurement and loss data maintenance.	Y
4.2.4	**Operational Risk Management Techniques** • The banks use an ORM framework. • The banks use incident loss data in order to be more proactive in taking action before an operational risk manifests itself.	Y
4.2.5	**Operational Risk Identification** • The responsibility for operational risk identification rests with the people who manage the processes and systems. • The main data sources to identify operational risks are the skill and experience of the people involved in the identification process. • Operational risks identification and appraising are done simultaneously. • The Audit Function was not involved in this incident since the Audit Function may provide valuable input to those responsible for ORM, but does not have direct ORM responsibilities.	Y
4.2.6	**Operational Risk Appraisal** • Operational risk estimation and evaluation are done concurrently. • The output from each phase has a different emphasis with one focusing on probabilities (estimation) and the other on at least financial impact (evaluation). • The responsibility for operational risk appraisal rests with the Managers in the Business Units. • The operational risk appraisal process is subjective or judgemental assessment of the probability and impact of the risk. • The main data source to appraise operational risks is the experience of the people involved in the process.	Y
4.3	**Operational Risk Mitigation**	
4.3.1	**Responsibility for Operational Risk Mitigation** • The responsibility for operational risk mitigation rests with the	Y

	Managers in the Business Units.	
4.3.2	**Operational Risk Mitigation – Exploring the Tactics Used** • The main operational risk mitigation tactics used are: 'Terminate', 'Treat', 'Take' and 'Transfer'.	Y
4.3.3	**Operational Risk Mitigation – Deciding What to Do** • The Managers in Business Units are responsible for deciding the mitigation tactic to deploy. • The process used in the selection of the appropriate mitigation tactic is informal and based upon the nature of the risk involved.	Y
4.3.4	**Operational Risk Mitigation – Barriers Faced by Management** • The main operational risk mitigation barriers are cost, resource, ignorance, customer reaction and reputation.	Y
4.4	**Operational Risk – Quantification and Training**	
4.4.1	**Quantification** • The responsibility for operational risk quantification rests with the Corporate Operational Risk Function.	N
4.4.2	**Training** • Training was seen as an important tool in all ORM phases.	Y

Key: Y = Yes, the critical incident tallies with the data analysis results of the study.
N = No, the critical incident data does not tally with the data analysis of the study.

Source: Developed by the author

Incident No. 18 – Deed Store

According to Basel II classification (Basel II, p. 257), this critical incident is an example of the sixth source of operational risk (see section 2.3.4.2): Business Disruption and Systems Failures - utility disruptions, software failures and hardware failures.

This incident came to light as a result of a competitor having a fire in their deed store with an associated cost of around AED 8 million. Following this incident, the risks and controls relating to the deed store in the bank were examined and it was discovered that the fire prevention system would not have worked had a fire occurred. The problem was traceable back to the halogen gas fire prevention system, which requires a certain pressure to be effective. It was discovered that this pressure did not exist, but the Business Unit

responsible for the deed store had already decided to remove this system and replace it with a water-based one, which requires no pressure to be maintained. However, because of costs and budget constraints, a decision was taken not to replace the halogen gas and at the same time a new conveyer belt was installed necessitating drilling a large hole in the wall directly into the store, which reduced the pressure even further. The Business Unit was unaware of the potential risk it had created, and the decision not to move forward to a water based system had not properly been communicated. The net result was the financial impact, had this risk occurred, would have been catastrophic (estimated at AED 18 million). There would also have been a significant impact on 20 members of the staff who worked in the area, as a result of the halogen gas fire prevention system being ineffective due to the hole that had been made for the conveyer belt.

The risk division became involved in mitigating the risk that now existed and a report was prepared for the Board recommending the installation of a sophisticated water-based system at a cost of around AED 1 million. The recommendation was accepted by the Board.

This is an example of 'Treat' being used to further reduce the likelihood of the operational risk occurring. In this particular case the risk had also been 'Transferred' (via insurance) but this would have been void because the problem with the pressure in the deed store had not been resolved.

This incident supports the data analysis findings because it highlights the importance of monitoring external events and stress testing them in the bank's own environment. The incident also confirms the escalation process that takes place in deciding upon the risk mitigation action (the scale and the cost of the mitigation action meant the final decision was taken at the Board level) and further emphasises the 'ignorance' constraint as one of the key problems facing management.

Table 33: Critical Incident No. (18) Data Analysis vs. Study Data Analysis

	Operational Risk Management Area	Conformance to the Data Analysis
4.2	**Operational Risk Management**	
4.2.1	**Defining Operational Risk** • The operational risk in this incident is included in the definition of operational risk.	Y
4.2.2	**Operational Risk Management in the Organisation** • Operational Risk Managers operate in the Business Units.	Y
4.2.3	**The Role of the Operational Risk Management Function** • The Corporate Operational Risk Function was not involved in this incident since the core responsibilities of the Corporate Operational Risk Function are: policy setting, aggregation of operational risk profile, high level reporting, assurance, framework setting, operational risk measurement and loss data maintenance.	Y
4.2.4	**Operational Risk Management Techniques** • The banks use an ORM framework. • The banks use key risk indicators to monitor operational risk. • The banks use incident loss data in order to be more proactive in taking action before an operational risk manifests itself.	Y
4.2.5	**Operational Risk Identification** • The responsibility for operational risk identification rests with the people who manage the processes and systems. • The main data sources to identify operational risks are the skill and experience of the people involved in the identification process. • Operational risks identification and appraising are done simultaneously. • Frequent monitoring of both potential operational risk sources and key risk indicators to assess existing operational risks. • The Audit Function was not involved in this incident since the Audit Function may provide valuable input to those responsible for ORM, but does not have direct ORM responsibilities.	Y

4.2.6	**Operational Risk Appraisal** • Operational risk estimation and evaluation are done concurrently. • The output from each phase has a different emphasis with one focusing on probabilities (estimation) and the other on at least financial impact (evaluation). • The responsibility for operational risk appraisal rests with the Managers in the Business Units. • The operational risk appraisal process is subjective or judgemental assessment of the probability and impact of the risk. • The main data source to appraise operational risks is the experience of the people involved in the process. • The external environment and loss data are other data sources to appraise operational risks.	Y
4.3	**Operational Risk Mitigation**	
4.3.1	**Responsibility for Operational Risk Mitigation** • The responsibility for operational risk mitigation rests with the Managers in the Business Units.	Y
4.3.2	**Operational Risk Mitigation – Exploring the Tactics Used** • The main operational risk mitigation tactics used are: 'Terminate', 'Treat', 'Take' and 'Transfer'.	Y
4.3.3	**Operational Risk Mitigation – Deciding What to Do** • The Managers in Business Units are responsible for deciding the mitigation tactic to deploy. • The process used in the selection of the appropriate mitigation tactic is informal and based upon the nature of the risk involved. • An escalation procedure existed in the banks when the Business Unit could not unilaterally decide on the course of action due to constraints.	Y
4.3.4	**Operational Risk Mitigation – Barriers Faced by Management** • The main operational risk mitigation barriers are cost, resource, ignorance, customer reaction and reputation.	Y
4.4	**Operational Risk – Quantification and Training**	
4.4.1	**Quantification** • The responsibility for operational risk quantification rests with the Corporate Operational Risk Function.	Y
4.4.2	**Training** • Training was seen as an important tool in all ORM phases.	Y

Key: Y = Yes, the critical incident tallies with the data analysis results of the study.
N = No, the critical incident data does not tally with the data analysis of the study.

Source: Developed by the author

As discussed above, in all the critical incidents and those in *Appendix* (C), the phases of ORM were in line with the data analysis findings. Further, the critical incident analysis results support the study data analysis findings; however, with very few exceptions.

4.8 Summary of Findings

The most significant finding of the research is that all of the banks in this study are developing their risk management framework in accordance with the requirements of the Basel II accord. There remains much to be done, however, on the measurement side of operational risk with all of the banks being in the embryonic stages of development. The study confirmed previous findings vis-à-vis the definition of operational risk. There is a common understanding of the broad areas that operational risk covers with strategic and reputational risks being excluded, as per Basel II definition of operational risk.

There are two types of Operational Risk Managers present in all banks: the Corporate Operational Risk Manager and the Business Unit Operational Risk Manager. The roles of the two appear to be clearly articulated and they have close working relations although there is no direct reporting line between them. This is not necessarily a problem but it highlights the issue of maintaining good communication channels between the individuals if both are to do their jobs efficiently (minimise any overlap) and effectively (sharing best practices). The same comments may be said of the relationship between the Operational Risk Managers and Internal Audit. The study found that the reporting lines of Internal Audit and the Corporate Operational Risk Function were identical in three of the banks.

This in turn could cause problems with independence, when Internal Audit has to review the work of the Operational Risk Function.

The study found that a risk-mapping framework was present in all of the banks, though the system was being piloted in Delta bank at the time the work was carried out. The phases within the framework were found to be consistent with the literature although there are a number of variations in the modus operandi and documentation produced reflecting the adapted development of these frameworks and the individual preferences of the banks. All the frameworks were used to manage as opposed to measure operational risk. Whilst the Corporate Operational Risk Functions were the owners of the framework, the responsibility for managing (identification, appraisal and mitigation) operational risk was found to be with the managers in the Business Unit, a responsibility that was in effect delegated down from the Board.

One of the key findings of the study is that managers in the Business Units rely on help from both internal and external specialists in discharging their responsibility. This is the case for all phases in the ORM process and again reflects the broad scope of what is defined as operational risk. Identifying when they need help and who can help them is a crucial element in the process.

Turning specifically to operational risk mitigation and the focus of this study, the findings indicate that the mitigation process for an operational risk varies from a simple improvement to an internal control procedure to the complexity of establishing a project

team to resolve the matter. The tactics used were found to be broadly in line with the literature of operational risk, which is principally found in an organisation's internal control environment (Basel II). Another important finding of the study is in relation to the barriers or constraints that exist in mitigating operational risk. While the issue of cost is unsurprising, more worrying is what was described as 'ignorance' or lack of awareness of operational risk. One of the key ways to improve this is through training and the study found that whilst there was widespread support for the development of formal training, very little had actually taken place.

The findings are particularly important in the context of the operational risks that contributed to Financial Crisis and Dubai Crisis, the impact on the UAE commercial banks and how to mitigate these risks in order to prevent recurrence of such crises in the future. The analysis shows that the focus of attention shall be imbedded ORM culture, health Corporate governance and the need for cutting-edge or robust risk management structures across credit, market and integrated ORM.

The cross-data analysis identified a number of emerging themes and differences between the banks. An important commonality is that the banks' operational risk frameworks are aimed at managing rather than measuring operational risk.
Despite some commonalities in approach, there were nonetheless some important differences. However, the differences tend to be variations on a theme rather than specific differences in approach.

Critical incidents were used to triangulate the study findings. The result shows that the phases of ORM were in line with the data analysis findings. Further, the critical incident data analysis supports the study data analysis findings.

This next section (Chapter 5) considers the implications of the findings of the study for the management and mitigation of operational risk in the UAE commercial banks.

5. ANALYSIS AND IMPLICATIONS FOR MANAGEMENT - STUDY CONCLUSIONS ABOUT THE RESEARCH PROBLEM

5.1 Introduction

This section considers the implications of the findings of the study (Chapter 4) for the management and mitigation of operational risk in the UAE commercial banks. The experiences of the managers from four of the leading banks involved in ORM are used to draw lessons for others who may be embarking on a similar path. This section opens with a discussion of the organisational implications, followed by an examination of the implications for Operational Managers, the Operational Risk Function and Internal Audit, the three main players identified in the management of operational risk. Finally, conclusions about the research problem are discussed and a proposed model is offered.

5.2 Organisational Implications

5.2.1 Implications for the Board

Evidence in this study indicates that UAE commercial banks are facing a changing external environment and that management will need to keep abreast of the changes that are occurring and the operational risks that they may bring. Part of the management process requires looking ahead, planning for expected and unexpected outcomes, organising adequate resources, and controlling the work done. The operational risks associated with the future intent of the bank in this turbulent environment, will require effective mitigation strategies. Management behaviour in dealing with these risks must take account of any delusions of control that may exist and the development of appropriate performance measurement systems to monitor operational risks will assume increasing importance.

This is a point endorsed by Masli and Peters (2009) and Hopkin (2010) whose studies of the relationship between risk management and organisational control indicate that a system of effective risk management can redirect the emphasis of control towards prevention rather than cure, and thus impact directly on the performance of the organisation.

Basel II placed risk management and internal control firmly on the agenda of the Board. The Boards of banks have a particular interest in managing operational risk because of the requirements to set aside capital to cover unexpected losses. Banks are unique in this respect and tying up capital in this way reduces the amount of money that is available for distribution to shareholders. There can be little doubt that the Board has an influential role in managing operational risk by creating a culture of risk awareness and distilling it down to the Operational Managers in the Business Units. The following comment from one of the managers seems to capture the context:

> "I believe you should start at the top, and have a clearly defined policy and then make sure that is properly understood, communicated down and adhered to in the business."

The Board carries the ultimate responsibility for the risk management activities that are undertaken. Previous high profile ORM failures (such as Barings, Société Générale, Indymac) have given rise to criticisms of Boards for their failures to establish effective internal control environments and monitor adherence to laid down procedures. Operational risk is embedded within a banks internal control environment (Basel II). It is a complex issue and the explicit management of operational risk will demand continuous Board

attention as risk profiles change due to changes in internal and external circumstances. The following comment from one of the managers seems to capture the mood:

> "I would probably suggest that a lot of the major operational losses occurred because management turned a blind eye."

Turning a blind eye never has been an excuse, and if it continues then it will remain an important cause for why operational risk incidents occur. So, what should Boards be doing to ensure that they are managing their risks effectively? The following comment from one of the managers seems to shed light on this area:

> "Boards should know their main risks."

This is probably the minimum that could be expected. If every member of the Board is unaware of the most significant risks that the bank faces, then their chances of being able to manage them effectively are severely diminished. Basel II outlines the criteria that Boards should be following. For example, Basel II proposes that banks should publicly, and in a timely fashion, disclose more detailed information about the process used to control their operational risks and the regulatory capital allocation technique they use. The financial reporting of risk was proposed to encourage better risk management, help reduce the cost of capital and provide enhanced reporting to investors.

The UAE commercial banking business involves more than just banking as has been noted in Chapter 2. All of the banks in this study, for example, have large insurance operations, which contribute to the banks' overall profitability and risk profile. The breadth of operations and, therefore, the breadth of operational risks, are large. Boards need to recognise this and ensure that they maintain sufficient expertise to understand and manage

these risks. A final consideration for the Board is the amount of money that the Bank spends or should spend on managing operational risk:

> "The Group spends virtually all their expenses on managing operational risk in one form or another whether it be by the Business or us centrally."

This observation from one of the Heads of Operational Risk suggests it is not just a question of the direct costs of the operational risk employees that should be considered, but a large amount of the bank's overall budget as everyone has a role to play in managing operational risk.

5.2.2 Risk Management Committee

As the results of the study have shown, the use of an ORM committee (or even a risk committee) to oversee operational risk is by no means consistent in the banks. There is little in the literature discussing operational risk committees (Spira and Page 2003). The breadth and newness of operational risk in relation to the UAE commercial banks appears to be a strong pointer towards establishing such a committee or including it within a generic risk management committee. Whilst the research did not examine this area in detail there are a number of issues arising from the study that are worthy of further consideration.

An ORM committee could normally be created as a sub-committee of the Board and could fulfill a number of roles in helping to manage and measure operational risk. For example, matters of policy may be decided, establishing the boundaries and categories of operational risk, overseeing key projects, deciding upon mitigation actions which span business units and receiving regular reports on operational risk. Where a risk committee is already in

existence, then there could be a strong argument for extending the terms of reference of this committee to include operational risk:

> "One of the problems with operational risk is that it literally covers the operation from beginning to end. In reality, all activities have operational risk elements in them."

Credit risks could be added to this, as there are operational processes involved in assessing the credit worthiness of an individual/organisation. Market risk could be added, too. Equally, the inclusion of the scope of operational risk in a generic risk management committee would help to ensure that all risks in the bank are being managed. Strategic and reputational risks within the context of operational risk remain the subject of some debate:

> "...it was all about getting management to see that what they thought was a really good strategy was actually flawed, and it's flawed not because it's not a good thing to do; it's flawed because you're not managing the operational risks that go with exactly what you are doing."

> "Turning around to a division and saying the next year we want to increase your volume by 200% has operational risks and quite often, what you will find is the operational risk has been assessed based on a static organic growth."

Whilst Basel II has specifically excluded strategic and reputational risks from the measurement debate, these still remain risks and as such need to be managed explicitly. This raises some interesting problems about whether strategic and reputational risks should be quantified. If not, then the 'holy grail' of being able to quantify a bank's total risk exposure will never be reached. If so, then the question is how should it be done?

The Risk Management Committee could also take an overall responsibility for the measurement of operational risk and the subsequent allocation of the capital set aside to

Business Units, thus reflecting the amount of operational risk they are carrying. This latter point is set to be a potential problem area unless a fair and reasonable method can be found to allocate capital.

Finally, the Risk Management Committee could help set the tone for ORM in the bank by ensuring that a consistent message is filtered down to the Business Unit. The results of the study indicate that the message behind good ORM is about being more operationally risk aware rather than being risk averse. This message can be communicated in a number of ways, including for example, training (see section 5.3.3).

5.2.3 The Operational Risk Manager

The research found that there are two types of Operational Risk Manager in the banks studied. These are the Corporate Operational Risk Manager and the Business Unit Operational Risk Manager. The roles have been well defined and there is evidence that the two work closely together. The Corporate Operational Risk Manager role has developed into the central monitoring role where a high level and aggregate view of the operational risks being faced by the bank can be assembled. Out of what appears to be a growing need to help the Business Unit improve its management of operational risk, the Business Unit Operational Risk Manager role has evolved. These managers are part of the Business Units and work with them on a day-to-day basis facilitating, helping and enticing the others into achieving the desired level of operational risk.

The existence of these roles in any organisation is confirmation of the explicit nature of ORM. They effectively add value by ensuring that the organisation manages the operational risks and not the other way round. As such, they are similar to the Internal Auditor: they are there to prevent something bad from happening. It was beyond the scope of this study to examine the skills and experience required to be an Operational Risk Manager but it is certainly a possible area for further research:

> "I think to do operational risk well; there is no substitute for having been an auditor first, preferably an Internal Auditor."

The author is not surprised that one of the Operational Risk Managers interviewed made this comment as Internal Auditors focus their efforts on the internal control systems where operational risks are principally found. The challenge for the Operational Risk Manager is in ensuring that the managers with whom he works understand the difference between his/her role and that of the Internal Auditor. This is particularly so where the reporting lines of both units are the same.

5.2.4 Integrated Risk Management

> "I think operational risk as a term has not really been widely used within the bank until it became much more popular in the last few years. Up until then the focus was certainly very much towards credit and market risks, although in reality, many of the issues about credit risk were actually operational risk issues."

> "We must take risks as a bank."

> "Banks are in the business of risk... ...at a price."

Risk management is an ongoing process and of fundamental importance to a bank because of the regulatory requirements in relation to capital. Therefore, it makes good sense to develop an approach to risk management which combines all the major forms of risk[66]: market, credit and operational. Whilst the nature of these risks may be different, operational risk is the common denominator as operational processes exist in both market and credit risk transactions. As a result, the boundaries are sometimes blurred.

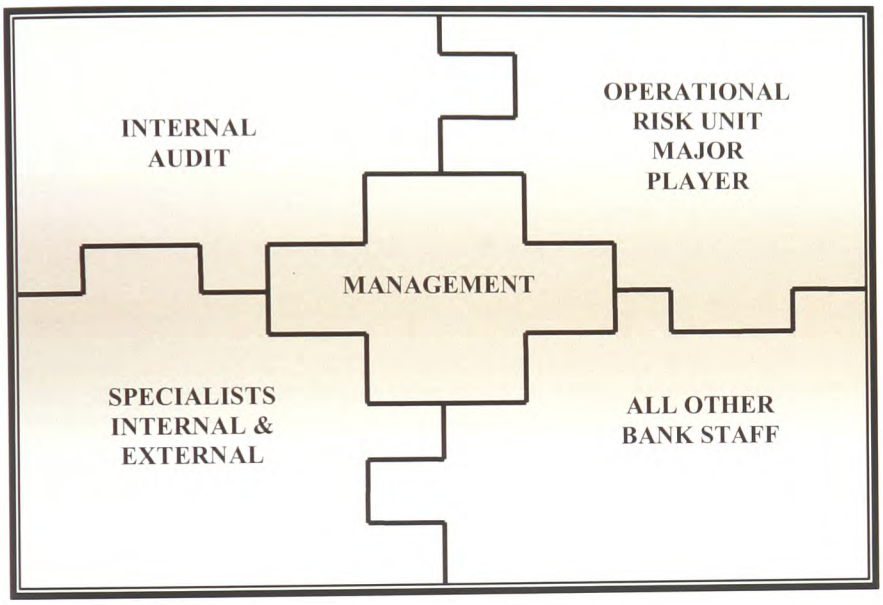
Developing an integrated risk management approach across credit, market and operational risk could be difficult to achieve because of the inherent differences in the nature of the three risks and ways in which they need to be managed, and, therefore, mitigated. Credit Risk Managers are proactive in performing up-front analysis of company and economic data (Kevin 2005), whilst market risk managers analyse risk in multiple transactions after they have been taken (Kevin 2005). Operational Risk Managers on the other hand assess the risk profiles of Business Units. Whilst it makes intuitive sense to have a similar reporting line, the approaches adopted to manage these risks will remain different.

One feature of operational risk that differs from credit and market risk is the number of people who have the opportunity to help manage it. The research indicates that everybody has a role to play since operational risk exists in every procedure used in the bank. This suggests that an integrated form of ORM is an objective worthy of further consideration. Looking at this from the point of view of the main players there would be five pieces of the

[66] The reader is reminded that there are other forms of risk inherent in banking activities such as liquidity risk. Many banks describe their positions on these risks in their annual reports.

'jigsaw puzzle' that would have to fit closely together for an integrated and effective approach to be adopted. This is shown in Figure 14.

Figure 14: Integrated Operational Risk Management



Source: Developed by the author

What are the drivers behind making the jigsaw fit together? Based on the study findings, the author would offer the following (see section 5.5):

- Developing cutting-edge or robust risk management structures across credit, market and operational risk in order to help ensure that the operational risks resulting from credit and market risks are captured and managed.
- Ensuring soundness of the corporate governance structure.
- Integrating operational risk conscious culture into the culture of the organisation via mandate, leadership and commitment from the Board.

- Monitoring the macroeconomic conditions, business environment, market and credit risk data, key risk indicators, and performing continuous internal control review.
- Focusing on proactive rather than reactive ORM.
- Defining a well designed and embedded risk appetite framework, specifying the bank's risk capacity (maximum risk tolerance) and risk appetite (desired risk tolerance) following the guidelines proposed by the Board.
- Reviewing the business critical risk challenges with ORM as a tool to drive the business objectives.
- Creating sustainable value from ORM by improving business performance and safeguarding business continuity.
- Complying with what regulators expect from the commercial banks, and transforming regulatory requirements for ORM into competitive advantage.
- Ensuring that the information presented to regulators and management is consistent
- Retaining experienced well-trained staff.
- Ensuring market confidence.
- Conducting stress testing on regular basis as directed by the regulators.

Most of these drivers will be the foundation to the operational risk model proposed in section 5.6.1.

5.3 Implications for Operational Management

5.3.1 Operational Risk Management

The research confirmed that the responsibility for ORM lies with the managers in the Business Unit, i.e. operational management.

> "The whole idea is that every risk within the organisation has a home and someone who is responsible for it."

Risk-mapping identifies the risk owner in the sense described above and has moved ORM from being informal and implicit to formal and explicit. In short, Operational Managers who have always managed operational risk as part of their day-to-day responsibilities, now find that they do it with a better understanding of the problems involved. It is vital that Operational Managers recognise the pivotal role they play in this process and the demands that are now being placed upon them when explicitly managing such a complex area. Some of the issues that have been identified in the study include:

1. The need to consider the effect that one risk can have on another – see *Appendix C*, critical incident no. 11;
2. The need to focus on managing the key risks and not the risks that Operational Managers like or find easy to manage;
3. The need to establish a well-defined risk appetite for the bank and the different business units;
4. The need to look for support (either internally or externally) when Operational Managers are unable to manage an operational risk by themselves;
5. The need to emphasise the vital role that other bank staff play in helping to manage operational risk on a day-to-day basis.

Operational risk-mapping is not a one-off exercise. It is a continuous process that must be done in addition to the ongoing management of the operational risks that are found the moment the manager sits at his desk. New operational risks can appear from a variety of sources:

> "Centralised processing, telephone banking, internet banking and mobile banking are all new operational risks."

Operational Managers must be alert to these new threats and react accordingly. The research also identified the opportunities that exist with ORM, particularly the opportunity to challenge the amount of control that is being exercised in relation to the risks involved. Control processes, which have been in place for some time, need to be continually reviewed and checked to make sure they are still valid and appropriate. Operational risks can be over-controlled (control inefficiency) as well as under-controlled (control deficiency). The challenge for the Operational Manager is balancing the two control elements.

Operational Managers also need to understand that they have a vested interest in creating an operational risk environment with a low level of residual risk. One of the drivers behind this is the capital charge that Business Units are likely to suffer since operational risk measurement has become firmly embedded in the bank. The allocation of capital should, in theory, reflect the riskiness of the Business Unit.

Finally, in focusing their attention on their operational risks the managers must recognise the importance of working within a defined frame of reference. Specifically, this is likely to be the Business Unit objectives. Their efforts to manage operational risk need to begin with an assessment of their objectives from a risk perspective and a clear understanding of how these risks are currently being managed.

By responding positively to the benefits offered by the risk-mapping framework, Operational Managers can help protect themselves from the dangers that ineffective ORM can bring. The critical incidents reported in *Appendix C* bear witness to some of the problems that can be caused when managements are unable to effectively mitigate operational risks.

5.3.2 Operational Risk Mitigation

The focus of this research has been in the area of operational risk mitigation and a number of findings have implications to Operational Risk Managers. Firstly, recognising that there are a number of different ways to mitigate an operational risk, although the most common, treating the risk, is likely to be the most appropriate given that most operational risks are embedded in the internal control environment. Secondly, their decision to mitigate will be constrained by a number of factors inherent in the way the organisation works and their own perception of the risk and knowledge of what can be done. Thirdly, mitigation is one area where other specialist units can have an important role to play in advising and implementing on the most appropriate course of action. Fourthly, the decision taken on how the risk will be mitigated should include an agreed action plan which is capable of

being monitored, as a basis for ensuring the desired level of residual risks is being achieved.

A checklist for mitigating operational risks has been drawn up by the author. This is shown in *Appendix E*. The reader should note that this checklist is based on the data analysis undertaken by the author and may be seen as a practical roadmap that may be used by managers when faced with an operational risk mitigation situation.

This checklist is seen as an important contribution since it offers practical recommendations to improve existing practice and is of use not only to the banks in the study but to others who wish to enhance their risk mitigation process.

5.3.3 Training

The author considers that training in ORM is an important challenge for banks. The research indicated that the managers felt that there was still work to be done in this area. The current informal training that is given via the risk-mapping exercise is only half of the story:

> "They, managers of business units, are all risk aware when we all sit around and have a discussion but they don't think it is necessary when they are doing their plans and budgets and that kind of thing."

The development of a formal training programme with the emphasis on operational risk awareness could be an important part of the bank's armoury in defending themselves against operational risks. The author would, therefore, contend that demonstrating a formal

training programme would be a great asset for the banks when dealing with regulators. The risk-mapping process relies on people throughout and it is their knowledge, skills and experience, which will determine the robustness of the results. Training in risk management should not, therefore, be seen as an 'optional extra' in the development of staff, but as a 'standard feature.'

Training may be focused and specific to the needs of management and staff within the bank. An important part of the process would be to ensure that the new starters are given sufficient training as part of their induction programme. The development of a training strategy in the area of operational risk would be a key factor in helping to:

> "...increase the acceleration rate of risk management knowledge."

5.4 Implications for the Operational Risk Function

5.4.1 Risk-mapping Framework

> "What we have got to be careful about in putting any process in place for operational risk is that you don't switch off the common sense. We have seen it in dealing. You give dealers appealing software to become a mathematical genius, but they will still lose money because they forget to think."

The above comment from an operational manager has an important message behind it. The risk-mapping processes that the banks in this study are installing, or have installed, are not designed to be used as 'checklists' for managing operational risks. All staff who contribute to the process must think 'outside the circle' particularly in the first phase of ORM where risks are being identified. Where workshops are used, the selection of a range of people

will help to remove risk bias and the skill of the facilitator in extracting the data from participants will be key to the success of the process.

The study found that the risk-mapping process itself is still relatively new within the banks studied. Once the risk map becomes a complete compendium of the operational risks faced by the banks, then the emphasis on the risk mapping process will move towards updating the risk profiles and capturing any new risks arising from, for example, major developments in the Business Unit and Financial Crises. As the ORM process matures, there is likely to be more emphasis placed on internal and external monitoring of the key risks and developments of the operational risk incident database. It is unlikely that a generic ORM framework will develop given the nature of those used in the banks studied and also the increasing developments in software applications for ORM. Of particular interest are the approaches at Gamma bank and Delta bank which request the risk to be documented in terms of event and causes.

> "What we are trying to do is give the Business Unit Managers a structure which they can break down and understand more."

The author was unable to establish if the risk-mapping process had been applied carte blanche across the banks being studied. For example, have the operational risks within the Corporate Operational Risk Function been mapped? Is there a role for Internal Audit to play in completing this task (see section 5.5.1)? Have the operational risks in Internal Audit been mapped? The evidence in this study suggests that these aforementioned functions play

a pivotal role in assisting operational management in managing their operational risks. If their work cannot be relied upon[67], a question mark must hang over the whole process.

5.4.2 The Role of the Operational Risk Function

The Operational Risk Managers, whether they operate at the Corporate or the Business Unit level, have an important role to play in maintaining an acceptable level of operational risk in the bank. The study found that the primary vehicle for arriving at this desired level was the implementation of an agreed action plan to mitigate the risk. If this is to be effective then a tracking procedure must be implemented. Gamma bank appeared to have the most comprehensive procedure:

> "The tracking procedure is essentially through the operational risk manager being alert to action plans and delivery dates on these action plans and prompting business areas where they may have passed these dates with nothing happening or not enough happening. We here at the centre are also able to take an overview of how these plans are being progressed and are in a position to escalate them where necessary to Executive level."

Operational Risk Managers must recognise the growing importance that will be placed on managing this follow-up process.

The role of the Operational Risk Function appears to be well defined in the banks studied and there is a degree of commonality in the functions they undertake. Nevertheless, good open communication channels need to be maintained with other units such as Internal Audit.

[67] Internal Audit were criticised over the Barings fiasco for not being resilient enough and Basel II found that Internal Audit was ineffective in many problem banking organisations.

5.4.3 Quantification

As is evidenced by this study and the literature review, the measurement of operational risk remains the biggest challenge for banks. Basel II has proposed three methodologies in this regard. The Heads of Operational Risk from the four leading UAE commercial banks interviewed in this study have assumed responsibility for developing and installing an appropriate methodology. Seeing the benefits of quantification further down the lines within the Business Unit is open to question. There is evidence in this study that, sometimes, those at the 'sharp-end' of ORM see the quantification debate as irrelevant to them.

The implications, both from the research and literature, for the Operational Risk Function is that they are likely to have to bridge the gap between expectations of the regulators and the expectations of the bank.

5.5 Implications for the Internal Audit

5.5.1 The Role of the Internal Audit

> "People take this comfort factor from saying Internal Audit are happy with the proposal."

The evidence from this study indicates that the Internal Audit function has an important role to play in the ORM, nevertheless, without direct involvement. As a function, it is charged with providing an independent opinion on the adequacy of the internal control

environment, which is designed to mitigate all risks. It is not just interested in operational risk mitigation but in all forms of risk mitigation. Much of its focus will be on auditing the adequacy of internal controls for ORM.

One of Internal Audit's responsibilities is auditing the work of all the Operational Risk Managers and how effectively they do their jobs:

> "...if you can't rely on operational risk management doing its job, all the reports that they produce for you are next to useless."

It could be argued that one of the most important risks a bank faces is having an inadequate ORM framework. The most logical unit that is in a position to form an opinion on this is the Internal Audit. Through its reporting line to the Audit Committee, it provides comfort to the Board that the ORM framework that is in place is adequate and appropriate for the needs of the bank. Basel II makes specific reference to the role of Internal Audit as being to conduct regular reviews of the ORM framework.

Whilst regular is not defined, it suggests that Internal Audit should plan to review the work of Operational Risk Function on an ongoing basis in order to help satisfy the bank and the regulatory requirements. Based upon the work undertaken in this study, the author has drawn up a checklist for use by Internal Audit when it reviews the work of the Operational Risk Function. This can be found in *Appendix D*.

The identical reporting lines of both the Corporate Operational Risk Function and the Internal Audit in three of the banks in this study are a potential source of difficulty. There

are two reasons for this. Firstly, it could easily lead to confusion in the eyes of auditees about the precise roles and responsibilities of the two functions. Secondly, it compromises the independence of Internal Audit when it is reviewing the work of other Operational Risk Function (since both functions have the same reporting line). This is a matter that Senior Management should consider carefully, particularly in light of Basel II requirements, which requires the Board to continually review its Operational Risk Function scope of work, authority and resources. Basel II emphasises the fact that the Internal Audit has an important role to play in ORM; nevertheless, it should not assume the responsibility of ORM.

5.6 Proposed Operational Risk Mitigation Model

The main research problem that the study set out to answer was:

How do the UAE commercial banks mitigate their operational risk exposures?

In formulating this question, the author was interested to see how the current practice of operational risk mitigation compares to theoretical models and the expectations of the regulators. The Regulators (Basel II) have emphasised that they will continue working with the industry on risk mitigation concepts. Further, the author had some early discussions with one of the UAE regulators in the CBUAE, and it was apparent that their focus was on providing guidance on how to manage and measure operational risk.

Against this background, the remainder of this section discusses a proposed model on operational risk mitigation, how the move from implicit to explicit ORM in the UAE

commercial banks has affected the pre-mitigation and mitigation phases of the ORM model and what problems exist in mitigating operational risk.

Based on the evidence from this study, the following can be stated about OR mitigation:

1. There is no single best way to mitigate operational risk (*based on contingency theory*);
2. Managers mitigate operational risk by diagnosing the risk and selecting an appropriate mitigation tactic based on their internal environment (*based on the theory of bounded rationality*) and their own perception/knowledge of risk (*based on prospects theory*).
3. The action managers take to establish the correct implementation of a mitigation tactic should enable the organisation to guarantee its residual level of operational risk to be in line with the organisation's risk appetite (*based on control theory*).
4. The implementation of a mitigation tactic should lead to improvements to the internal control environment and a reduction in the level of operational risk (*based on complexity theory*).
5. Any mitigation actions should address first the cause of an operational risk and not only the event itself (*based on complexity theory*).

The author has argued that ORM in the UAE commercial banks has moved from being implicit to explicit. Such change in emphasis is important in building a model to illustrate the above conclusions because, whilst there are a number of key phases with implicit ORM, additional components may be added to demonstrate explicit ORM. The study has

found that these components, however, are not just limited to the mitigation phase of ORM, but are also found in the pre-mitigation phases. Looking at the mitigation phase in isolation would not give the whole picture and the author has, therefore, proposed a model which considers all the phases and components.

The proposed model will be presented in two complementary parts in order to shed more light on the related components:

1. Core ORM framework – shown in Figure 15.
2. ORM model including implicit and explicit phases, with the Core ORM Framework embedded – shown in Figure 16.

Further, the resulting ORM cycle is depicted in Figure 17.

5.6.1 Proposed ORM Model

The analysis of the results in this study indicates that ORM is at the core of a bank's operations, necessitating the integration of the ORM practices into all processes, systems and the bank's culture. The value of ORM is in supporting and challenging the Board to align the business control environment with the bank's strategy by measuring and mitigating operational risk exposure for optimal contribution to return for the stakeholders.

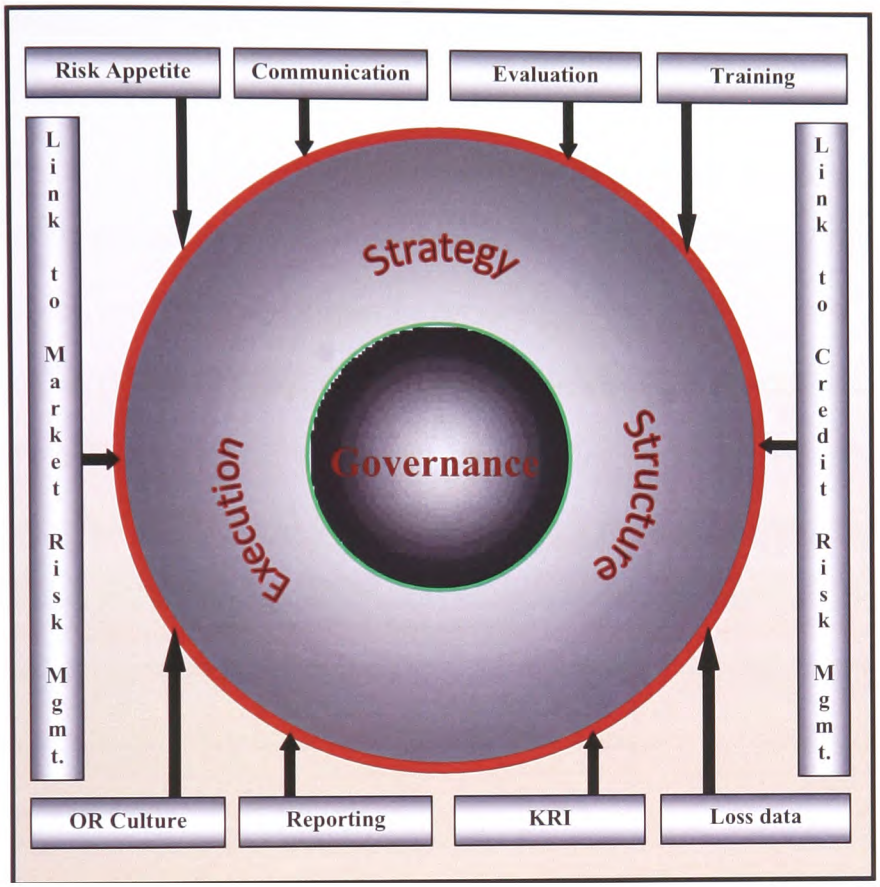
It further indicates that ORM keeps its people up-to-date on problems that have happened to other banks, allowing them to take a more proactive approach. The goal is to make the employees look at ORM as a business stakeholder and a shareholder, involve them at all

levels and bring stability into their jobs. However, and to start with, a bank needs to implement an ORM framework that encompasses all sources of potential risks as outlined by Basel II (see section 2.3.4.2).

5.6.1.1 Proposed Core ORM Framework

As noted earlier, there is no 'one-size-fits-all' approach to ORM framework since every bank needs to follow a framework that is specific to its own internal operating environment. The implication is that there is no 'standard' standard. Ultimately, the operational risk framework should not merely be Basel-compliant; it should also provide the bank with mechanisms for improving the overall operational risk culture and behaviour towards ORM. Based on the analysis of the study results, the author proposes the Core ORM framework shown in Figure 15.

Figure 15: Proposed Core ORM Framework



Source: Developed by the author

The proposed Core ORM framework consists of the following core, main and other important components:

5.6.1.1.1 Core Components

- **Governance:** It is the process by which the Board defines key objectives for the bank and oversees progress towards achieving those objectives. It defines the overall operational risk culture in the organisation, and sets the tone as to how a bank implements and executes its ORM strategy. A successfully executed

operational risk strategy often results in operational risk culture being firmly embedded in the vision, strategies, tools, and tactics of the organisation. Governance sets the precedence for Strategy, Structure and Execution.

- **Strategy:** A bank's strategy for operational risk drives the other components within the ORM framework and provides clear guidance on operational risk appetite or tolerance, policies, and processes for day-today ORM.
- **Structure:** When designing the ORM framework structure, the bank's overall operational risk scenario should serve as a guideline, including initiatives like laying down a hierarchical structure that leverages current operational risk processes and developing operational risk measurement models to assess regulatory capital vis-à-vis the actual operational risks confronted. Centralised aggregation of operational risk information collected across the organisation, further, provides useful insight for the desired hierarchical structure. The implementation of these concepts allows operational risks to be handled consistently throughout the organisation.
- **Execution:** Once the ORM framework structure has been established by an organisation, adequate procedures should be designed and implemented to ensure execution of and compliance with these policies at Business unit level. The first step includes identification of the operational risks inherent in the day-to-day processes of the bank. After the identification of the inherent operational risks, target tolerance limits of these risks should be established; an activity which is commonly accomplished by calculating the probability (estimation) of materialisation of the operational risks, by considering the drivers or causes of the

risks together with the assessment of their impact (evaluation). In the proposed ORM model, the estimation and evaluation will be referred to together as diagnosis. The result of the operational risk diagnosis process enables the bank management to compare the operational risks with the bank's operational risk strategy and policies, identify those operational risk exposures that are unacceptable to the bank or are outside its operational risk appetite, and select and prioritise appropriate mechanisms for mitigation selection and implementation.

5.6.1.1.2 Main Components

- **Risk Appetite Strategy:** A sound ORM framework ensures that the organisational behaviour is driven by its operational risk appetite. Adopting an operational risk strategy aligned to operational risk appetite leads to informed business and investment decisions.
- **Communication:** An organisation's top management must identify, assess, decide, implement, audit and supervise their strategic operational risks. There should be a strategic policy at the Board level to focus on managing operational risk at all levels and conscious efforts should be made to ensure that these policies are communicated at all levels and across the entire value chain.
- **Periodic Evaluation Based on Internal and External Environments:** A robust ORM framework puts the improvement of operational risk performance on a competitive level with other important mission concerns, while periodically evaluating the ORM performance goals in light of the internal and external factors.

- **Training:** The development of a formal training programme with the emphasis on operational risk awareness is an important part of the bank's armoury in defending themselves against operational risks.
- **Operational Risk Conscious Culture:** An operational risk conscious culture must be integrated into the culture of the bank, and this will need to include mandate, leadership and commitment from the Board. The Board must translate risk strategy into operational objectives, and assign risk management responsibilities throughout the organisation. It should support accountability and reward, thus promoting ORM efficiency at all levels.
- **Reporting (Disclosure) – External and Internal:** A bank should publicly and internally, and in a timely fashion, disclose more detailed information about the process used to control their operational risks and the regulatory capital allocation technique they use. The financial reporting of risk is key to encouraging better risk management, helps reduce the cost of capital and provides enhanced reporting to investors.
- **Key Risk Indicators and Loss Data:** These are important tools that enable the bank to monitor operational risk in order to be more proactive in taking action before an operational risk manifests itself.

5.6.1.1.3 Other Important Components:

- ✓ Establishing effective linkage with credit risk and market risk managements in order to manage the operational risks resulting from credit and market risks. There are operational processes involved in assessing the credit

worthiness of an individual or organisation. Meanwhile, market risk managers analyse risk in multiple transactions after they have been taken. Both of these activities have their associated operational risks.

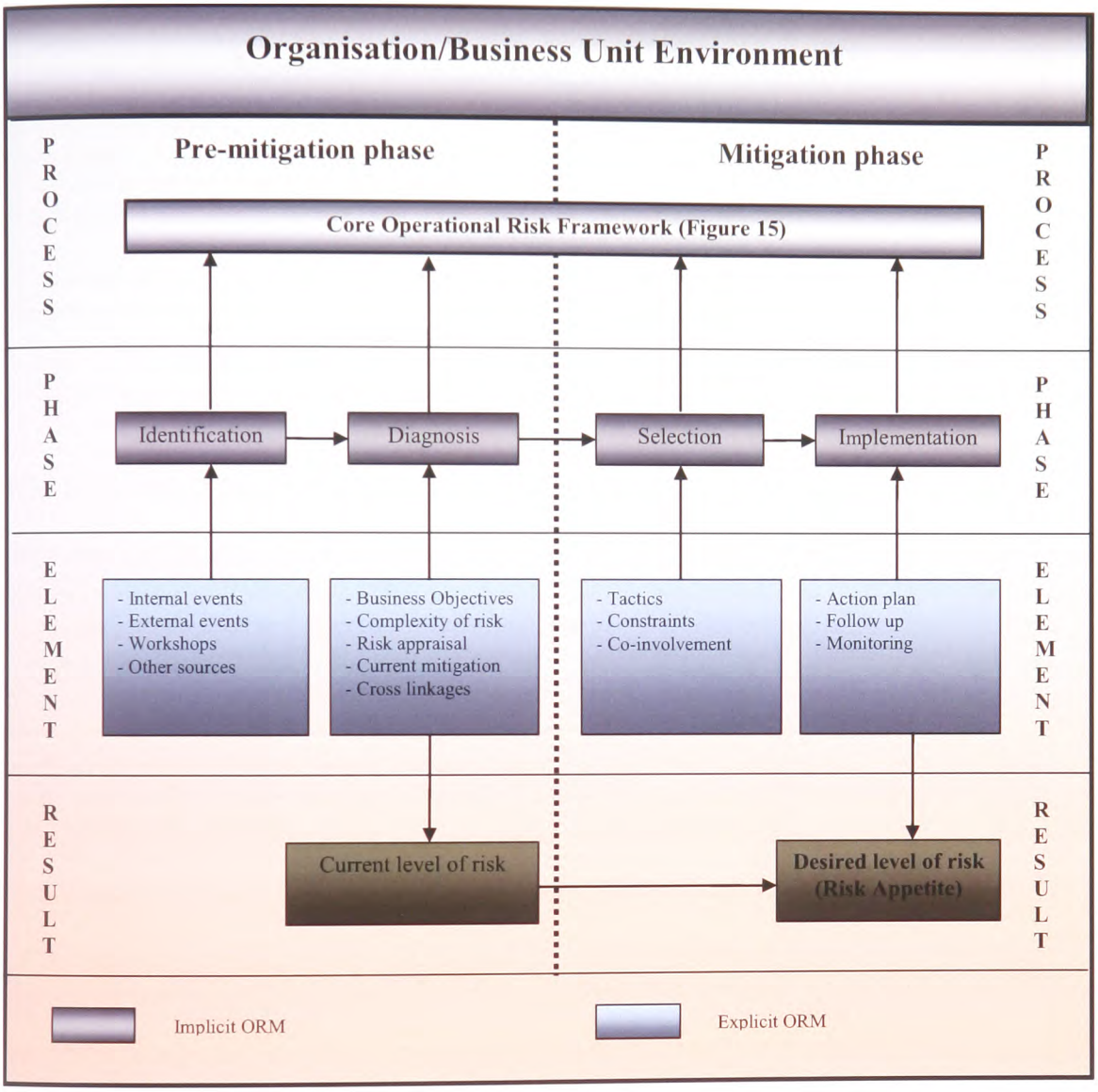
- ✓ Ensuring compliance with the regulatory requirements;
- ✓ Monitoring the macroeconomic conditions and business environment
- ✓ Conducting regular stress testing.

These components (section 5.2.4) play an important role in the overall ORM process in order to ensure that the operational risks are predicted, kept under control and mitigated in a timely manner.

5.6.1.2 Embedding the Core ORM Framework into the Proposed Overall ORM Model

The proposed ORM model with implicit and explicit phases is shown in Figure 16.

Figure 16: Proposed ORM Model with Implicit and Explicit Phases



Source: Developed by the author

The components of implicit ORM are shown as dark-shaded boxes along the horizontal line marked 'Phase'. These equate to the phases in the simple risk management model (see Figure 1) as per Table 34.

Table 34: Phases of the Risk Management Models Compared

Proposed ORM Model Phase	Simple ORM Model Phase
Identification	Identification
Diagnosis	Estimation, Evaluation
Selection	Mitigation
Implementation	Mitigation

Source: Developed by the author

With the arrival of explicit ORM, the implicit components have been augmented by a number of additional components which are represented by further three horizontal lines:

- Process – the core operational risk framework is the driver behind the whole ORM effort and the processes are embedded within it;
- Elements – each of the phases has a number of distinct elements which act as the main driver for that phase;
- Result – there is an explicitly stated current level of operational risk and desired level of operational risk (risk appetite).

Turning to the two pre-mitigation phases:

1. Identification – the evidence from the study indicates that there is a combination of elements which support this phase. Operational risks are identified through the examination of internal and external events (incidents/losses) via a number of sources (workshops, questionnaires, and so on) specific to the bank;

2. Diagnosis – the diagnosis of the risk is a crucial input into the mitigation phase and represents the assessment, which provides management with information pertinent to the current level and impact of risk. Evidence from the study points to a number of elements being used to arrive at the diagnosis: the objectives of the Business Unit, the complexity of the risk, the risk appraisal (probability/impact), the current mitigants in place and the cross linkages that the risk may have to other risks.

Turning to the mitigation phase:

1. Selection – the decision phase when the manager examines the risk diagnosis and selects, from the options available to him, what action to take. The evidence from the study suggests that the elements that will influence his decision are the tactics available to him, the constraints imposed upon him by the bank, his own knowledge of ORM, and his knowledge of who may be able to help him to mitigate the risk;
2. Implementation – the evidence from the study indicates that this final phase, the one that guarantees the desired level of operational risk, is driven by the establishment of an action plan (based on the mitigation tactic selected), the use of adequate follow-up procedures and the ongoing monitoring of operational risk key risk indicators.

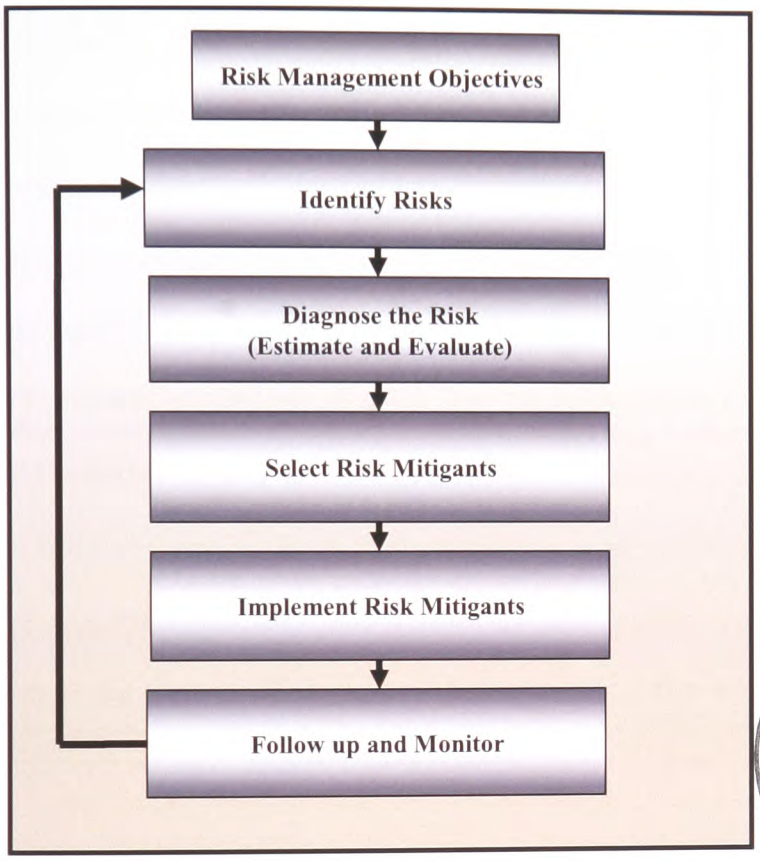
The reader will note that the model is in line with other decision-making models being a process for making logically sound decisions by following an orderly path from problem identification through to solution and is, therefore, well-rooted in existing theory (see Simon (1997) and Robins and Timothy (2008), section 2.2.3.)

It is the opinion of the author that the development of an explicit system to manage and, therefore, mitigate operational risk should be based on a model of this type. The reader is again reminded that operational risk is a large and complex area and to reduce its management down to a few boxes in a model is not intended to trivialise the task ahead but merely to identify the building blocks from which a tailored solution to the bank's own particular circumstances may be constructed. The model represents core practice derived from four of the leading UAE commercial banks.

5.6.2 Operational Risk Management Cycle

Based on the proposed model, the resulting ORM cycle is depicted in Figure 17.

Figure 17: Operational Risk Management Cycle



Source: Developed by the author

Even with such a process in place, it should not be assumed that the universal remedy to ORM has been found. Drawing on the evidence from the four banks in this study, a number of issues relating to operational risk mitigation were noted:

1. The diagnosis of operational risk is not a straightforward process. In some cases there may be observed or historical information upon which the impact/probability appraisal may be carried out whilst in others there may be next to nothing, for example;

2. Any mitigation actions should address the cause of an operational risk and not only the event itself. Taking a simple example, having insufficient stocks of marketing material for customers should be due to lack of stock-checking procedures. In this case the solution is not to order more marketing material but to introduce improved stock checking controls;
3. Undertaking the cost/benefit analysis that is used to help decide on whether or not to mitigate a risk, is not always an easy task. For example, should the risks associated with web-site security breaches consider the reputational losses that the bank could suffer? If so, how should they be quantified?
4. Ensuring that managers are alert to the possibility of using help in mitigating an operational risk relies heavily on the individual judgement of the manager and his willingness to call for help. These types of factors may be difficult to manage because they rely on individual behaviours and personal relationships.

5.7 Summary and Conclusions about the Research Problem

This Chapter discussed the implications of the findings of the research for the bank management. Operational risk is a complex area and the problems inherent in managing it are spread across the whole of the bank's operational processes. Lessons learnt from this study of four major UAE commercial banks have been used to illustrate some of the issues that the bank management have to face in addressing how best to manage, and with it, mitigate operational risk. Implications for the organisation, operational management, the Operational Risk Function and Internal Audit were discussed.

The starting point is the Board that must set the risk appetite not just for operational risk, but for all risks that the bank has to face. The Board is ultimately accountable for the operational risk exposures that the bank faces and although it delegates this responsibility to Operational Managers, it must retain a firm grip and understanding of what is already a fast evolving area.

The study found that the use of a Risk Management Committee to oversee operational risk is not consistent in the banks. Such Committee could be created as a sub-committee of the Board and could fulfill a number of roles in helping to manage and measure operational risk: matters of policy, overseeing key projects, mitigation actions which span business units and receiving regular reports on operational risk.

Credit risks could be added to this bouquet of activities, as there are operational processes involved in assessing the credit worthiness of an individual or organisation. Equally, market risk managers analyse risk in multiple transactions after they have been taken. Both of these activities have their associated operational risks. The inclusion of credit and market risks in the scope of the Risk Management Committee would help to ensure that all major risks in the bank are being managed.

The Risk Management Committee could also take an overall responsibility for the subsequent allocation of the capital set aside to Business Units, thus reflecting the amount of operational risk they are carrying. Further, the Risk Management Committee could help

set the tone for ORM in the bank by ensuring that a consistent message is filtered down to the Business Unit.

The research found that there are two types of Operational Risk Manager in the banks studied: the Corporate Operational Risk Manager and the Business Unit Operational Risk Manager. The roles have been well defined and there is evidence that the two work closely together.

The existence of these roles in any organisation is confirmation of the explicit nature of ORM. They effectively add value by ensuring that the organisation manages the operational risks and not the other way round. Further, in focusing their attention on their operational risks, the managers must recognise the importance of working within a defined frame of reference. Specifically, this is likely to be the Business Unit objectives.

Some of the issues in ORM were identified. The research also identified the opportunities that exist with ORM, particularly the opportunity to challenge the amount of control that is being exercised in relation to the risks involved.

The focus of this research has been in the area of operational risk mitigation and a number of findings have implications to Operational Risk Managers. Firstly, recognising that there are a number of different ways to mitigate an operational risk, although the most common, treating the risk, is likely to be the most appropriate. Secondly, managers' decisions to

mitigate will be constrained by a number of factors inherent in the way the organisation works and their own perception of the risk and knowledge of what can be done. Thirdly, mitigation is one area where other specialist units can have an important role to play in advising and implementing on the most appropriate course of action. Fourthly, the decision taken on how the risk will be mitigated should include an agreed action plan which is capable of being monitored, as a basis for ensuring the desired level of residual risks is being achieved.

A checklist for mitigating operational risks has been drawn up by the author. This checklist is seen as an important contribution since it offers practical recommendations to improve existing practice and is of use not only to the banks in the study but to others who wish to enhance their risk mitigation process.

The research indicated that the development of a formal training programme with the emphasis on operational risk awareness could be an important part of the bank's armoury in defending themselves against operational risks. The author would, therefore argue that demonstrating a formal training programme would be a great asset for the banks when dealing with regulators.

The study found that the risk-mapping process itself is still relatively new within the banks studied. Once the risk map becomes a complete compendium of the operational risks faced by the banks, then the emphasis on the risk mapping process will move towards updating the risk profiles and capturing any new risks arising from, for example, major developments in the Business Unit and Financial Crises. As the ORM process matures,

there is likely to be more emphasis placed on internal and external monitoring of the key risks and developments of the operational risk incident database.

The Operational Risk Managers, whether they operate at the Corporate or the Business Unit level, have an important role to play in maintaining an acceptable level of operational risk in the bank. The study found that the primary vehicle for arriving at this desired level was the implementation of an agreed action plan to mitigate the risk, as cited above; however, the action plan needs to be coupled with an effective tracking procedure.

As is evidenced by this study and the literature review, the measurement of operational risk remains the biggest challenge for banks. There is evidence in this study that, sometimes, those at the 'sharp-end' of ORM see the quantification debate as irrelevant to them. The implication for the Operational Risk Function is that they are likely to have to bridge the gap between expectations of the regulators and the expectations of the bank.

The evidence from this study indicates that the Internal Audit function has an important role to play in the ORM, nevertheless, without direct involvement. As a function, it is charged with providing an independent opinion on the adequacy of the internal control environment, which is designed to mitigate all risks.

Based upon the work undertaken in this study, the author has drawn up a checklist for use by Internal Audit when it audits the work of the Operational Risk Function.

Based on the evidence from this study, some operational risk mitigation conclusions were drawn. These conclusions were associated with the theoretical foundation discussed in the literature review: *contingency theory* (section 2.1.2), *bounded rationality theory* (section 2.2.4), *prospects* theory (section 2.3.3) and *control theory* (section 2.3.4.4.1). Emphasis is placed on the fact that any mitigation action should address first the cause of an operational risk and not only the event itself.

The study found that operational risk is the common denominator between credit, market and operational risks; as operational processes exist in both market and credit risk transactions. However, developing an integrated risk management approach across credit, market and operational risk could be difficult to achieve because of the inherent differences in the nature of the three risks and ways in which they need to be managed and, therefore, mitigated. On the other hand, the study also indicated that everybody in the organisation has a role to play in ORM since it exists in every procedure used in the bank. This suggests that an integrated form of ORM is an objective worthy of further consideration. The drivers behind an integrated ORM were identified and used to propose an ORM framework.

The study has found that the implicit and explicit components of ORM are not just limited to the mitigation phase of ORM, but are also found in the pre-mitigation phases, and the author has, therefore, proposed a model which considers all the phases and components. The model consists of a 'Core' part (focusing on governance, strategy, structure and execution and other components) and an overall ORM model with the 'Core' embodied,

including the implicit and explicit components, employing the integrated ORM drivers concluded from this study.

Based on the proposed overall ORM model, the resulting ORM cycle was concluded. However, even with such a process in place, it should not be assumed that the universal remedy to ORM has been found.

To conclude, sound corporate governance should be at the heart of the ORM framework; with well designed strategy, structure and execution processes. Appropriate operational risk mitigation and internal control procedures should be established by the business units such that residual operational risks are mitigated to the acceptable level. Regular reviews must be carried out, to analyse the control environment and test the effectiveness of implemented controls, thereby ensuring that the business operations are conducted within acceptable operational risk limits. It is essential that the Board ensures consistent monitoring and controlling of operational risks, and that operational risk information is received by the appropriate people, on a timely basis, in a form and format that will aid in the monitoring and control. Stress testing and operational risk Key Risk Indicators should be established to ensure timely warning is received prior to the occurrence of an event. Key to effective KRI's lies in setting the threshold at the acceptable level of operational risk. The execution and implementation of an integrated ORM framework is key to setting up effective ORM environment ensuring that the business is conducted within appropriate operational risk tolerance limits.

The final word in this section is left with one of the managers interviewed and his view on the value of ORM.

> "The real value of what is emerging with operational risk management is the recognition that it is not wrong to have an operational risk exposure, as long as you understand it and can say it's not cost effective to the business to introduce more controls."

6. SUMMARY OF THE RESEARCH

6.1 Summary of the Research

Operational risk is a new topic in the UAE commercial banking industry and this research examined the management of operational risk specifically in the UAE commercial banks. The study was focused on the mitigation phase of ORM where a number of key issues were reviewed: the responsibility for operational risk mitigation; the tactics that were used to mitigate an operational risk and the barriers that existed when deciding upon an appropriate operational risk mitigation strategy. The subject is highly topical in the UAE banking industry because of the regulatory requirements vis-à-vis operational risks that were proposed by Basel II, the Financial Crisis and Dubai Crisis. The research looked at operational risk from the perspective of the Risk Manager, the Operational Manager in the Business Unit and the Internal Auditor and may thus be described as inter-disciplinary.

The literature review in Chapter 2 provided a high level overview of some of the theoretical propositions and current issues in the areas of Management and Organisation, Banking, and Internal Audit that are of relevance to ORM. ORM has become an important issue for the regulators and the banks themselves in each of these areas. Basel II accord, the upcoming Basel III and the regulatory regime were discussed in Chapter 2 along with a review of the theory in the generic area of risk management, with a section dedicated to operational risk. An important distinction was made between the management of operational risk and the measurement of operational risk, both of which are seen as important by the regulators.

One of the drivers of this research was the early discovery by the author that little academic research had been done in the area of operational risk for financial services organisations in the UAE. On top of this, the regulators had begun to apply pressure on the UAE commercial banks to effectively manage operational risk and the Internal Audit profession was also moving their audit approach towards being 'risk based'. These were the initial impetuses for the research, and further endorsement was given by the Financial Crisis and Dubai Crisis, which have moved operational risk towards the top of the agenda for bank management.

The research design is described in Chapter 3. A case study approach was adopted as offering the best opportunity to answer the research questions. The design is qualitative and is based upon well-established techniques for case study research, particularly when the topic is new, the area has had no prior research (relating to the UAE commercial banking industry) and the research aims to build a model. Four cases were selected for study. Each case represents an example of a major player in the UAE commercial banking arena, a point that was important in the selection criteria, as the research was targeted at establishing best practices by looking at industry leaders.

The major findings of the research, summarised in Chapter 4, are that all of the banks in this study are developing their ORM frameworks in accordance with the requirements of the Basel II Accord. There remains much to be done, however, on the measurement side of operational risk with all of the banks being in the embryonic stages of development. The

study found that a risk-mapping framework was present in all banks though the system was being piloted in one at the time the work was carried out.

The phases within the frameworks were found to be consistent with the literature although there are a number of variations in the modus operandi and the documentation produced reflecting the tailored development of these frameworks and the individual preferences of the banks. All the frameworks were used to manage as opposed to measure operational risk.

Turning specifically to operational risk mitigation and the focus of this study, the findings indicate that the mitigation process for an operational risk varies from a simple improvement to an internal control procedure to the complexity of establishing a project team to resolve the matter. There was general agreement that the barriers or constraints to mitigating operational risk are driven by either cost or ignorance. Whilst the issue of cost is unsurprising, more worrying is 'ignorance' or lack of awareness of operational risk. One of the key ways to improve this is through training and the study found whilst there was widespread support for the development of formal training, very little had actually taken place.

The study has made a number of important contributions which may be summarised as follow:

- Operational risk is acknowledged as being under researched in the UAE commercial banking industry and the study has helped to chart and clarify some of

the practical applications of ORM processes as well as proposing a model for the management of operational risks;

- Whilst the study focused on the UAE commercial banks, the findings and implications of the research have international applications because BCBS, as the primary regulator in this area, is an international organisation responsible for setting, and ensuring compliance with, bank regulations;
- The operational risk that contributed to the Financial Crises, how these risks were mitigated and what should be done to prevent recurrence of these crises, from the perspective of the UAE commercial banking industry, were investigated. This is an important contribution and has implications in the UAE and at international level.
- The results of the study suggest that in some areas of operational risk mitigation the process is still immature in the UAE commercial banks. For example, the mitigation of operational risks which span the business units had no well defined and accepted process. This is an important contribution and provides the impetus for carrying out further targeted research;
- Current practices are defined in the research, and the checklist emerging from these practices provides practical advice and prescriptive recommendations about what can be done to mitigate an operational risk exposure;
- The evidence from the study suggests that Internal Audit role, another area which is acknowledged as being under-researched, is a crucial element in the management of operational risk. However, the Internal Audit shall not be responsible for ORM. The high level review document for auditing the Operational Risk Function is based on

the findings of the study and contributes to the independent appraisal of the function required by Basel II;

- Studying the ORM process should assist banks to reduce their exposures and help to promote a more risk aware climate, where losses are minimised and cash flow enhanced;
- The study contributes to a better understanding of the risk management processes required and demanded under reporting initiatives, particularly in the UAE context with the CBUAE requirements;
- Methodologically, the study increases and contributes to the growing repository of case study research programmes in the generic area of risk management.

Practicing managers, whether they are in Risk Management, operational Management or Internal Audit should benefit from a number of the implications arising from the research. This in turn should lead to improvements at the organisational level as the firm becomes more aware of the causes of operational risk and the potential effects that they could have if adequate mitigation strategies are not put in place.

6.2 Limitations of the Research

One of the main limitations of the research was the lack of prior research in the area of operational risk in the UAE commercial banks due to the embryonic nature of the subject in the UAE. The author had to mainly revert to available literature on operational risk although it was not directly related to the UAE commercial banking industry.

Operational risk in banking is a sensitive subject and access to individual bank data is difficult, specifically in the UAE where reputational issues can be a major concern. Also, confidentiality of the subject makes replication of the studies more difficult.

The broad nature of operational risk means that not all contextual factors have been considered in depth. For example, the use of IT support systems to manage and mitigate operational risk was not discussed thoroughly with the interviewees. This is, however, seen as a fruitful area for further research.

6.3 Suggestions for Further Research

There are a number of areas that the author has cited in the thesis that could usefully be examined by further research studies.

The use of qualitative techniques to develop the ORM model meant that further research could be undertaken to generalise the findings. This generalisation could be done across the broad area of financial services in the UAE or, alternatively, could be done across a broader spectrum of banks (such as Islamic banks). The replication of the study in this way would provide valuable insights into how the financial service industry as a whole is tackling ORM and mitigation.

The establishment of operational risk units and the systems that support them are still in the early days but further work could usefully be carried out on the costs involved. How much are banks willing to spend? How was the expenditure thus far incurred justified? What do

managements perceive the expected benefits to be of their investment in ORM? Is the cost merely viewed as another regulatory cost?

There is an opportunity to explore further the relationship between ORM (the art) and operational risk measurement (the science). In theory there should be a high degree of correlation between the two, i.e. the better the management the lower the figure for quantified operational risk, and vice versa. This presents a particularly interesting opportunity for further research.

The relationship between operational risk and shareholder value presents an opportunity for further study. A capital charge for operational risk will have an effect on the required rate of return and, by definition, the value that may be created or destroyed. The explicit nature of ORM should, in theory, improve an organisation's cash flow by reducing potential losses thus providing a direct benefit to shareholder value. Additionally, if more explicit disclosure on how operational risks are being managed are presented in the Annual Report, then it would suggest that the market is 'better informed' about the organisation, a fact that should be taken into account in setting the share price.

The effective use of IT packages and Decision Support Systems in ORM systems is an area still under development where an important contribution could be made. It is important to establish how these systems are developed in banks and other financial services organisations and to what use they are being put. The integration of a system, which is able

to both 'manage' and in some way 'measure' the risks, would provide a significant step forward in the future management of operational risk.

The personal characteristics, skills and experience of individuals who have to manage operational risk present an opportunity for further study. These factors are important points to recognise, since ultimately it is people who have to manage operational risk in an organisation.

Mobile banking (mBanking) is a new trend in the UAE commercial banks. There is one drawback; that is, with technology comes risk and in particular operational risk that needs to be addressed as early as possible. The literature review reveals that operational risks in mBanking have not been researched and, hence, can be an interesting area for future research.

The need to better understand bank risk-taking incentives and the implications of adopting new products and processes, as well as the need to better understand the relationship between competition and risk are under researched areas and recommended for further research.

The literature review revealed that there is notable clustering of cases of bank failure (in a country) around a few years rather than an even spread over time. The presence of clusters could be an indicator that the state of the macro economy is a contributory factor in bank failures. This presents an interesting opportunity for further research.

Stress testing applied to the UAE commercial banks is an area that has not been explored. The testing is conducted under assumptions of deteriorating economic conditions, such as low Gross Domestic Product, higher unemployment rate and lower real estate prices. The purpose of the test is to ensure that banks have enough capital to survive.

Finally, BCBS published its third Capital Accord in December 2010: "*International Framework for Liquidity Risk Measurement, Standards and Monitoring- Basel III*" in response to the deficiencies in the financial regulation revealed by the Global Financial Crisis from liquidity risk perspective. The enforcement of Basel III and the consequent implications for ORM can be an interesting area for further future research.

APPENDICES

Appendix A: The Credit Card Fraud Case - a Case Study

This incident is useful to examine because it is in the public domain, has a significant impact and provides a perfect opportunity to examine the mitigating tactic used.

The data for this case study has been obtained from one of the managers interviewed and the press (GulfNews, Sep. 16, 2008 issue, and critical incident number 1 cited in *Appendix C*) and illustrates an operational risk that affected the public who used credit cards issued by some of the UAE commercial banks in 2008. This incident represents an operational risk, where the final cost was estimated at hundreds of millions of AED.

Introduction

In 2008, some of the UAE commercial banks noted excessive international use of customers' credit cards, coupled with some customer complaints that their credit card statements were carrying sums that were not used by them. Upon contacting samples of the customers whose cards have been excessively used, it turned out that most of these customers neither left UAE nor used their credit cards internationally. The Authorities and regulators were called upon to investigate the situation. The results of the investigation revealed that the concerned credit cards were hacked as follows:

A customer uses his credit cards via his Personal Identification Number (PIN) to access his account details, withdraw cash and make purchases at an Automatic Transaction Machines (ATM) or a Points of Sale (POS). The ATM or POS communicates with computers on a network used by the banks to execute the transaction.

1. The computers on the network process the information sent to them from the ATM or POS to locate the bank that the account belongs to, verify that the customer is authorised to access the account and execute the transaction.
2. Hackers break into the network and insert programmes which capture the customer's account information and PIN while being processed.
3. Using the captured information, hackers duplicate the credit card to withdraw cash and make purchases on the customer's accounts.

The incident illustrates the 'External Fraud' type of the operational risks as classified by Basel II. The scale and complexity of the problem meant that the Authorities, the Regulators and the Banks themselves all became involved in the actions that followed. These actions, which have fallen principally on the banks involved, have necessitated a complete review of the banks' networks and computer technicalities with compensation payments made where customers lost money due to this kind of external fraud.

What are the operational risks involved?

With the benefit of hindsight, it was very easy to be wise about the operational risks that were either not identified or identified and ignored, i.e. no appropriate mitigation action was taken. From the data that has been collected on this case the following appear to have been the key operational risks that ultimately led to the external fraud being highlighted:

1. Banks involved did not comply with the IT safety recommendations related to using advanced anti-hacking programmes (firewalls);

2. Banks involved did not have a mechanism to verify the international transaction with the credit card holder at the time of transaction execution;
3. There was an emphasis on producing quantity of business (credit card holders were incentivised to excessively use their credit cards internationally);
4. Supervisory controls within the banks involved were ineffective in detecting the problem at an earlier stage.

Another important operational risk to emerge has been the reputational risk of the banks involved. Only time will tell if public confidence in using credit cards internationally has been permanently dented by the debacle.

Mitigating the risks involved

Much of the work done on the credit card fraud case has been concerned with compensating affected customers (Take the risk). Further, the following mitigants (Treat the risk) were employed:

1. Temporary restriction of international ATM and POS usage by credit cards.
2. Deployment of powerful anti-hacker firewalls on all concerned computers and networks.
3. Immediate cancellation and replacement of the involved credit cards.
4. Establishment of setups by the banks to verify the credibility of international credit card transactions (by calling the concerned user or sending him a short message on his mobile phone at the time of the transaction.)

The involvement of so many high profile players has meant that some mitigating actions are almost being imposed on the Business Unit Managers. The tactics are, therefore, aimed at risk reduction, specifically looking at reducing the probability of the event recurring.

Given the current estimates of this fraud case (AED 300 million), it is one example of an operational risk that cannot be allowed to happen again.

Table 35: Credit Card Fraud Critical Incident Data Analysis vs. Study Data Analysis

	Operational Risk Management Area	Conformance to the Data Analysis
4.2	**Operational Risk Management**	
4.2.1	**Defining Operational Risk** • The operational risk in this incident is included in the definition of operational risk.	Y
4.2.2	**Operational Risk Management in the Organisation** • Operational Risk Managers operate in the Business Units.	Y
4.2.3	**The Role of the Operational Risk Management Function** • The Corporate Operational Risk Function was not involved in this incident since the core responsibilities of the Corporate Operational Risk Function are: policy setting, aggregation of operational risk profile, high level reporting, assurance, framework setting, operational risk measurement and loss data maintenance.	Y
4.2.4	**Operational Risk Management Techniques** • The banks use an ORM framework.	Y
4.2.5	**Operational Risk Identification** • The responsibility for operational risk identification rests with the people who manage the processes and systems. • The main data sources to identify operational risks are the skill and experience of the people involved in the identification process. • Operational risks identification and appraising are done simultaneously. • Frequent monitoring of both potential operational risk sources to assess existing operational risks. • The Audit Function was not involved in this incident since the Audit Function may provide valuable input to those responsible for ORM, but does not have direct ORM responsibilities.	Y

4.2.6	**Operational Risk Appraisal** • Operational risk estimation and evaluation are done concurrently. • The output from each phase has a different emphasis with one focusing on probabilities (estimation) and the other on at least financial impact (evaluation). • The responsibility for operational risk appraisal rests with the Managers in the Business Units. • The operational risk appraisal process is subjective or judgemental assessment of the probability and impact of the risk. • The main data source to appraise operational risks is the experience of the people involved in the process.	N
4.3	**Operational Risk Mitigation**	
4.3.1	**Responsibility for Operational Risk Mitigation** • The responsibility for operational risk mitigation rests with the Managers in the Business Units.	N
4.3.2	**Operational Risk Mitigation – Exploring the Tactics Used** • The main operational risk mitigation tactics used are: 'Terminate', 'Treat', 'Take' and 'Transfer'.	N
4.3.3	**Operational Risk Mitigation – Deciding What to Do** • The Managers in Business Units are responsible for deciding the mitigation tactic to deploy. • The process used in the selection of the appropriate mitigation tactic is informal and based upon the nature of the risk involved.	N
4.3.4	**Operational Risk Mitigation – Barriers Faced by Management** • The main operational risk mitigation barriers are cost, resource, ignorance, customer reaction and reputation.	Y
4.4	**Operational Risk – Quantification and Training**	
4.4.1	**Quantification** • The responsibility for operational risk quantification rests with the Corporate Operational Risk Function.	Y
4.4.2	**Training** • Training was seen as an important tool in all ORM phases.	Y

Key: Y = Yes, the critical incident tallies with the data analysis results of the study.
N = No, the critical incident data does not tally with the data analysis of the study.

Source: Developed by the author

Appendix B to the Case Study Protocol

Appendix B1: Semi-structured Interview Questions

Notes:

1. The questions in normal type were the main questions, whilst those in small type were supplements to the main questions.
2. The type in italics were 'triggers' drawn up by the author and were used as prompts, where necessary, to try and elicit a response.

PART 1: A

What is operational risk?

1. What is the bank's definition of operational risk?
2. Is the definition documented?
3. Who approved the definition of operational risk? Based on what?

   (Board, Executive Committee, Audit Committee, Risk Management Committee, Other Committee – Which? Individual – Who?)
4. Which risks are included in your definition of operational risk (define each type)?

   Internal fraud.
   External fraud.
   Employment practices and workplace safety.
   Clients, products and business practice.
   Damage to physical assets.
   Business disruption and systems failures.
   Execution, delivery and process management.
   Legal risk.
   Strategic risk.
   Reputational risk
   Environmental risk.
   Others
5. What do you know the history of operational risk and how the term came about?
6. How was operational risk managed in the past in your bank?
7. Do you have any idea how much your bank spends on managing operational risk Cost of the department, training, consultants, etc ?
8. What do you think about what the regulators are trying to do with operational risk?

   (Valuing operational risk, liaison with them, etc.)
9. Does your operational risk unit have terms of reference? Could I have a copy?
10. In terms of impact, do major operational risks have an owner to focus management

attention?

11. Why was the operational risk unit established and how was the structure determined?

PART 1: B

The Risk Management Framework

Risk Identification: is the process of perceiving hazards, identifying failures and recognising adverse consequences.

1. Who is responsible for identifying operational risk exposures?
2. Is this responsibility clearly laid out in their job function?
3. Describe the process by which operational risks are identified.
   (physical inspection, check lists, flow-charts, audit reporting, Management reporting, incident reporting)
4. How frequently are these processes used?

Risk Estimation: is the process of estimating risk probabilities, describing the risk, quantifying the risk.

5. Does the bank estimate operational risk exposures?
6. Who is responsible for estimating operational risk exposures?
7. What approach is used?
8. What is your roadmap for AMA implementation?
9. Describe the process by which operational risks are estimated.
10. Are there set criteria used to assess the exposure?
11. What data is used to estimate the risk?
12. Are the benefits of accepting the risk examined?
13. How is the risk judged as being acceptable or otherwise?

Risk Evaluation: is the process of evaluating the impact of the risk, judging acceptability of the risk, comparing risks against benefits.

14. Does the bank evaluate the impact of operational risk exposures?
15. Who is responsible for evaluating the impact of operational risk exposures?
16. Describe the process by which operational risks are evaluated.

17. Are there set criteria used to assess the impact?

18. What data is used to evaluate the impact?

PART 2: A

Who mitigates operational risk?

1. What is the organisational structure of the bank?
2. Are there clearly identifiable business units?
3. What is the level of autonomy?
4. Within this structure who mitigates operational risk?
5. What is the structure of the Risk Management Unit?
6. Do they have approved Terms of reference?
7. Do they mitigate operational risk?
8. What is the structure of the Internal Audit unit?
9. Do they have approved Terms of reference?
10. Do they mitigate operational risk?
11. Are External Consultants used to mitigate operational risk?
12. Why and when are External Consultants used?
13. Are other internal Units used to mitigate operational risk?
14. How do the areas included in the definition of operational risk relate to the Units responsible for mitigation – Who mitigates what?
15. To what extent will the Business Unit Management call upon additional support given the pressures they are under?

    When an operational risk exposure is identified what tactics are used to mitigate the risk?

Avoidance (i.e. making the occurrence of the event impossible)?

a) Under what circumstances avoidance would be used?

b) Establish the types of risks that are/ have been mitigated this way (e.g. deliberately withdrawing from a market because the operational risks involved are considered to be too great)

Reduction/Suppression (i.e. reducing the likelihood of occurrence of the event and/or reducing eventual loss)?

a) Under what circumstances would risk reduction/suppression be used?

b) Establish whether the following tactics are used:

(Improving internal control procedures, redesigning the processes involved, training, separation of Personnel, ongoing monitoring (audit/compliance/reviews), improved reporting systems, external advice ,improving quality standards)

***Assumption/Retention** (i.e. accepting the likelihood of the occurrence of the event and undertaking no mitigating actions)?*

a) Under what circumstances would risk assumption/retention be used? Is there a monetary limit used to guide the decision?

b) Establish the types of risks that are/ have been mitigated in this way (e.g. level of loss and probability of occurrence is considered to be low)

***Insurance** (i.e. accepting the likelihood of the occurrence of the event but reducing the eventual loss by transferring the risk)?*

a) Under what circumstances would risk insurance be used?

b) Establish the types of risks that are/have been mitigated this way (e.g. business interruption risks are frequently insured)

***Combinations** (of the above techniques)?*

a) Under what circumstances would a combination of techniques be used?

b) Establish the types of risks that are/have been mitigated this way (e.g. risks mitigated through the establishment of a captive insurance company)

***Others**?*

a) Under what circumstances would other techniques be used?

b) Establish the type of risks that are/have been mitigated in this way.

16. How are the mitigation tactics chosen and put into action?
17. Who decides the action to be taken?
18. Why is that person/function responsible for making the decision?
19. What procedures are in place to select a course of action? (Is OpVAR used as part of the data for making a decision?)
20. What procedures are in place to implement a course of action?
21. How do you ensure that the mitigation tactic is working?
22. What follow up procedures are in place?
23. Who carries out the follow- procedures?
24. Why is that person/function responsible for carrying out the follow-up procedure?
25. If the mitigation tactic is not deemed to be working satisfactorily, what procedures are

in place to correct this?

26. Does that person/function carrying up the follow-up work have the authority to enforce changes?
27. How frequently are follow-up reviews undertaken?
28. What are the barriers to mitigating operational risk?

Political barriers: *Organisational inertia, culture, risk maturity.*

Economic *– Lack of cash, lack of other resources, impact on the bottom line.*

Ignorance *– Staff training, Inadequate communication about risk exposures, "It will not happen to us" syndrome, unawareness of possible options.*

Others *- Practicality of the tactic involved, effect on the internal organisation – resistance to changing practices, effect on the external environment – reputation could be harmed, Government regulations, monitorability of the required action, required action not deemed to be effective in the timescale involved, (for example, because of changing environmental circumstances.)*

PART 2: B

Critical Incidents: A recent example of an operational risk incident.

1. Who was involved in the discussions about how to solve it?
2. What actions were considered to mitigate the risk?
3. Who decided on what action to take?
4. Why did that person decide?
5. Why were certain tactics rejected?
6. How successful has the mitigation action been?
7. How was it followed up?
8. How representative is this incident of the risk mitigation process within the business?
9. Do you have any other examples of where the risk mitigation action was different?
10. Why was a different action taken?

Note: Discuss the credit card fraud case as a fall back example.

PART 3

The Financial Crisis and Dubai Crisis

1. Could you predict the Financial Crisis and Dubai Crisis? How can the recurrence of these Financial Crises be predicted and mitigated in a timely manner?
2. What are the operational risks that contributed to the Financial Crisis and Dubai

Crisis?

3. What is the impact of the Financial Crises on your bank?
4. How were the operational risks that contributed to the Financial Crisis and Dubai Crisis mitigated in your bank?
5. Have you conducted stress testing in your bank? Are you planning for stress testing?

AppendixB2: Coding System

Operational Risk Case Studies – Coding System

AREA	CODE	NOTES
Internal Organisation	**IO**	
IO: Operational Risk Definition	IO-ORD	Definitions of operational risk that are used by the banks
IO: Operational Risk AREAS	IO-ORA	Areas that are included within the definition
IO: Risk Management Structures	IO-RMS	Comments/perceptions relating to the bank's risk management structure
IO: Risk Management Policy	IO-RMP	Comments/perceptions relating to the bank's risk management policy
IO: Organisation Structure	IO-OS	Comments/perceptions relating to the bank's organisational structure
IO: General Information	IO-GI	General information about the bank/risk management that helps to put the study into context
IO: Training	IO-TRAIN	Comments relating to risk management training within the organisation
IO: Risk Strategies	IO-START	Current strategies for dealing with risk management within the organisation
IO: Database	IO-DBASE	Information relating to the use of a risk management (incident) database within the organisation
Operational Risk Identification	**RI**	
RI: Responsibility	RI-RES	Comments on responsibility for operational risk identification
RI: Process	RI-PRO	Information on the sequence of events that lead to operational risk being identified
Operational Risk Evaluation	**REV**	
REV: Responsibility	REV-RES	Comments on responsibility for operational risk evaluation
REV: Process	REV-PRO	Information to the sequence of events that lead to operational risk being evaluated
REV: Data	REV-DATA	Types of data used in the operational

		risk evaluation process
REV: Quantification	REV-QUAN	Information on the use of quantification risk measurement techniques
REV: Judgement	REV-JUDGE	Indications of the ways of thinking that caused a decision on operational risk evaluation to be made
Operational Risk Estimation	**RES**	
RES: Responsibility	RES- RESP	Comments on responsibility for operational risk estimation
RES: Process	RES- PRO	Information on the sequence of events that lead to the impact of the operational risks being estimated
RES: Data	RES- DATA	Types of data used in the operational risk estimation process
RES: Judgement	RES- JUDGE	Indications of the ways of thinking that caused a decision on operational risk estimation to be made
Operational Risk Mitigation	**RM**	
RM: Business Unit	RM-BU	Comments on the Business Unit role in operational risk mitigation
RM: Internal Audit	RM- IA	Comments on the Internal Audit role in operational risk mitigation
RM: Risk Management	RM- RM	Comments on the Risk Management role in operational risk mitigation
RM: External Consultants	RM-EC	Comments on the External Consultants role in operational risk mitigation
RM: Other Units	RM-OU	Comments on role of other internal units in operational risk mitigation
RM: Interfaces	RM-INTER	Information describing the collective way in which operational risk is mitigated
RM: Barriers	RM-BAR	Information on the barriers to mitigating operational risk
RM: Critical Incidents	RM-CRI	Reported incidents on operational risk
Operational Risk Mitigation Tactics	**TAC**	
TAC: Avoidance	TAC-AVOID	Evidence to support avoidance being used as an operational risk mitigation tactic
TAC: Reduction/Suppression	TAC-RED	Evidence to support reduction/suppression being used as an

		operational risk mitigation tactic
TAC: Assumption/Retention	TAC-ASS	Evidence to support assumption/retention being used as an operational risk mitigation tactic
TAC: Insurance	TAC-INS	Evidence to support insurance being used as an operational risk mitigation tactic
TAC: Combination	TAC-COMB	Evidence to support combination of the above being used as an operational risk mitigation tactic
TAC: Other	TAC-OTHER	Evidence to support other techniques being used as an operational risk mitigation tactic
Operational Risk Mitigation Procedures	**PROC**	
PROC: Decision Maker	PROC-DM	Comments on who decides on the course of action to be taken when an operational risk is being mitigated
PROC: Selection process	PROC-PRO	Information relating to the process of selecting a suitable mitigation tactic.
PROC: Implementation	PROC-IMP	Information relating to the process used in implementing a selected mitigation tactic
PROC: Corrective Action Tracking	PROC-CAT	Information relating to the subsequent follow-up of implemented operational risk mitigation decisions
General	GEN	
GEN: Quotations	GEN-QUO	Noteworthy quotations for responsible use in the report
GEN: Regulators	GEN-REG	Comments related to the regulators including their role in operational risk mitigation
GEN: Report	GEN-REP	Items for possible inclusion in the report
Critical Incidents	**CI**	
CI: Decision maker	CI-DEC	Information about the decision maker in the critical incident
CI: Action	CI-ACT	Information concerning the action taken in the critical incident
Financial Crisis and Dubai Crisis	**FCDC**	
FCDC: Prediction	FCDC-PRD	Comments on the prediction of the

		Financial Crisis and Dubai Crisis.
FCDC: Prevention	FCDC-REC	Comments on the prevention of the recurrence of the Financial Crisis and Dubai Crisis.
FCDC: Contribution	FCDC-OR	Comments on the operational risks that contributed to the Financial Crisis and Dubai Crisis.
FCDC: Impact	FCDC-IMP	Comments on the impact of the Financial Crisis and Dubai Crisis on banks.
FCDC: Mitigation	FCDC-MIT	Comments on the mitigation of the Financial Crisis and Dubai Crisis.
FCDC: STRESS	FCDC-STR	Comment on stress testing.

Appendix B3: Case Study Report

Case Study Report: Bank Alpha

Bank Specific Details	
Name of the bank	Alpha
Number of branches	64 in UAE and 24 international
Established	1967
Net profit for the year 2009	AED 1 billion
Net profit for year 2010	AED 803 million
Total Assets for year 209.	AED 94.3billion
Total Assets for year 2010.	AED 84.8 billion
Number of employees	1824
OR current approach	BIA

Introduction: Operational risk is an area that is not researched in the UAE, and is of growing importance to financial institutions because of regulatory requirements. The study examines an uncharted area in the UAE with a practical orientation towards managing operational risk on a day-to-day basis. The researcher aims at building a research model that would be of interest and use to policymakers, regulators and those in charge of the banking corporate governance. In particular, this model is expected to contribute to the area of operational risk mitigation in the banking sector.

How do the UAE commercial banks mitigate their operational risk exposures?	
Definition of Operational Risk	
Source of definition	Adapted Basel II
Specific risk exclusions	Market, credit
Level of understanding	Good
Operational Risk Management in the Organisation	
Corporate OR unit reporting lines	Group Risk
Internal Audit reporting lines	Group Risk
Relationship: OR vs. Internal Audit	Very close
Size of Corporate OR Unit	5 persons
Establishment of Corporate OR Unit	2008
Use of Business Unit ORM	Developing,4 Persons
Business Unit ORM reporting lines	Local Management
Relationship: Business Unit ORM vs. Corporate OR unit	Close
OR Committee	No
Other OR roles	None
Role of Corporate Operational Risk Function	
Policy setting	Yes
Monitoring function	Implicit in role
Scope of role	All operational risks

Custodians of the framework	Yes
Assurance on 'key' risks	Yes
Aggregating OR's	Yes
Mitigating OR's which span the Business Unit	Coordinate effort
Maintenance of loss data base	Yes
Corporate Operational Risk Unit works with Business Unit ORM	Often
Corporate Operational Risk Unit works with Business Units	Often
ORM Techniques	
Framework in place	Yes
Type of approach	Top down and Bottom up
Extent of coverage	50% completed
Change management projects	Several processes
Loss database	Yes
Key risk indicators (KRI's)	Yes
Framework – Data Output	
Business Unit	
Objectives	No
Materiality threshold	Yes
Identification	
Risk – description	Yes
Risk – event/cause	No
Risk category	Yes
Recording whether the risk has been experienced	Yes
Assessment	
Likelihood	Yes
Financial impact	Yes
Consequential impact	Yes
Mitigation	
Assessment of controls in place	Yes
Indicators to monitor	Yes
Action plans	Not formal
Implementation date	No
Operational Risk Identification	
Responsibility	Business Unit
Support	When required
Focus	Management concerns
Instrument	Framework
Process	Workshop Material events Networking Software Scenario analysis. Risk indicators Internal audit process
Data source	People Internal loss data Specialised organisations
Output	List of risks
Operational Risk Appraisal	
Responsibility	Business Unit

Support Instrument Process	When required Framework Workshop
Likelihood focus Impact focus	Probability: 1 - 5 scale AED 1 to 5 scale with 6 scenarios
Data sources	People Current mitigants Historical data External environment Software Specialised organisations
Output	Business Unit Risk profile Risk measures
Operational Risk Mitigation	
Responsibility	Business Unit
Support	When required
Factors influencing support	Control issue Complexity of risk Option to share risk
Mitigation – Tactics	
Terminate	Yes New product
Treat	Yes Process improve New technology Tightening rules Contingency plans
Take	Yes Barrier present
Transfer	Yes Insurance
Other	Sharing
Mitigation: Selection Procedures and follow up	
Decision Maker Escalation Factors	Mainly Business Unit Scale of risk Cost of action Proposed tactic Approval limits
Selection process Factors	Informal Nature of risk Priorities Amount of work Others involved
Follow-up	Informal at Business Unit level
Mitigation – Barriers	
Main barriers	Cost and resource Ignorance Reputation No solution Organisation

Also noted	Politics
Related matters	-
Quantification	
Methodology	BIA
Time frame for AMA	3 - 5 years
Level of support	Skeptical about value of results
Training	
Approach	Formal
Method	Risk- mapping Framework
Focus	Management and staff
Operational Risk and the Financial Crisis and Dubai Crisis	
The Financial Crises were predictable	Yes
Recurrence Prevention Measures	Robust risk management structures Stress testing OR aware culture Improved corporate governance Effective regulation
Operational Risks that Contributed to the Financial Crises	Large credit growth Reactive ORM strategies Lack of risk appetite framework Weak regulatory framework
The Impact of the Financial Crises on the UAE Commercial Banks	Bad debt accumulation Lack of liquidity for lending Loss in asset value Loss of faith in the banking system Withdrawal of foreign depositors' money
Mitigation of the Operational Risks that Contributed to the Financial Crises	Intervention of the CBUAE by: Supplying liquidity Guaranteeing depositors' money Guaranteeing interbank lending
Stress testing	Not done yet. Planned during the next year.

Case Study Report: Bank Beta

Bank Specific Details	
Name of the bank	Beta
Number of branches	18 in UAE and 3 international
Established	1979
Net profit for the year 2009	AED 3.3 billion
Net profit for year 2010	AED 3.5 billion
Total Assets for year 209.	AED 125.5billion
Total Assets for year 2010.	AED 140.8billion
Number of employees	956
OR current approach	BIA

Introduction: Operational risk is an area that is not researched in the UAE, and is of growing importance to financial institutions because of regulatory requirements. The study examines an uncharted area in the UAE with a practical orientation towards managing operational risk on a day-to-day basis. The researcher aims at building a research model that would be of interest and use to policymakers, regulators and those in charge of the banking corporate governance. In particular, this model is expected to contribute to the area of operational risk mitigation in the banking sector.

How do the UAE commercial banks mitigate their operational risk exposures?	
Definition of Operational Risk	
Source of definition	Adapted Basel II
Specific risk exclusions	Market, credit
Level of understanding	Good
Operational Risk Management in the Organisation	
Corporate OR unit reporting lines	Group Risk
Internal Audit reporting lines	Deputy CEO
Relationship: OR vs. Internal Audit	Close
Size of Corporate OR Unit	6 persons
Establishment of Corporate OR Unit	2006
Use of Business Unit ORM	Developing, 3 Persons
Business Unit ORM reporting lines	Local Management
Relationship: Business Unit ORM vs. Corporate OR unit	Close
OR Committee	Part of risk committee
Other OR roles	None
Role of Corporate Operational Risk Function	
Policy setting	Yes
Monitoring function	Yes
Scope of role	All operational risks
Custodians of the framework	Yes
Assurance on 'key' risks	Yes

Aggregating OR's	Yes
Mitigating OR's which span the Business Unit	Coordinate effort
Maintenance of loss data base	Yes
Corporate Operational Risk Unit works with Business Unit ORM	Often
Corporate Operational Risk Unit works with Business Units	Often
ORM Techniques	
Framework in place	Yes
Type of approach	Bottom up
Extent of coverage	One cycle completed
Change management projects	Framework
Loss database	Yes
Key risk indicators (KRI's)	Yes
Framework – Data Output	
Business Unit	
Objectives	Yes
Materiality threshold	Yes
Identification	
Risk – description	Yes
Risk – event/cause	No
Risk category	Yes
Recording whether the risk has been experienced	Yes
Assessment	
Likelihood	Yes
Financial impact	Yes
Consequential impact	Yes
Mitigation	
Assessment of controls in place	Yes
Indicators to monitor	Yes
Action plans	Not formal
Implementation date	Yes
Operational Risk Identification	
Responsibility	Business Unit
Support	When required
Focus	Business U nit objectives
Instrument	Framework
Process	Workshop Material events Product development. Internal forums Questionnaires Risk indicators Networking Software Scenario analysis. Internal audit process
Data source	People Internal loss data Specialised organisations
Output	List of risks

Operational Risk Appraisal	
Responsibility	Business Unit Corporate Operational Risk Function
Support Instrument Process	When required Framework Workshop Internal audit process: challenging
Likelihood focus Impact focus	Probability: % AED: figure
Data sources	People Current mitigants Historical data Specialised organisations
Output	Risk rating
Operational Risk Mitigation	
Responsibility	Business Unit
Support	When required
Factors influencing support	Control issue Complexity of risk Cost effectiveness Potential impact Business Unit skills lacking
Mitigation – Tactics	
Terminate	Yes New product
Treat	Yes Process improve New technology Segregation of duties Automating checks Good controls
Take	Yes Cost/benefit
Transfer	Yes Insurance
Other	-
Mitigation: Selection Procedures and follow up	
Decision Maker Escalation Factors	Mainly Business Unit Scale of risk Cost benefit Level of change Technology impact Customer impact
Selection process Factors	Informal Nature of risk Current controls Tracking
Follow-up	Informal at Business Unit level
Mitigation – Barriers	

Main barriers	Cost Ignorance Reputation System fragilities Commercial pressures Customer reaction Establish priorities
Also noted	-
Related matters	-
Quantification	
Methodology	BIA
Time frame for AMA	3 - 5 years
Level of support	Worth doing, but still a lot to do.
Training	
Approach	Informal
Method	Risk- mapping Framework
Focus	Management
Operational Risk and the Financial Crisis and Dubai Crisis	
The Financial Crises were predictable	Yes
Recurrence Prevention Measures	Robust risk management structures Stress testing OR aware culture Improved corporate governance Effective regulation
Operational Risks that Contributed to the Financial Crises	Large credit growth Reactive ORM strategies Lack of risk appetite framework Weak regulatory framework
The Impact of the Financial Crises on the UAE Commercial Banks	Bad debt accumulation Lack of liquidity for lending Loss in asset value Loss of faith in the banking system Withdrawal of foreign depositors' money
Mitigation of the Operational Risks that Contributed to the Financial Crises	Intervention of the CBUAE by: Supplying liquidity Guaranteeing depositors' money Guaranteeing interbank lending
Stress testing	Not done yet. Planned during the next year.

Case Study Report: Bank Gamma

Bank Specific Details	
Name of the bank	Gamma
Number of branches	79 in UAE and 9 international
Established	1968
Net profit for the year 2009	AED 3.1 billion
Net profit for year 2010	AED 3.7 billion
Total Assets for year 209.	AED 190.6 billion
Total Assets for year 2010.	AED 211.3 billion
Number of employees	3753
OR current approach	BIA

Introduction: Operational risk is an area that is not researched in the UAE, and is of growing importance to financial institutions because of regulatory requirements. The study examines an uncharted area in the UAE with a practical orientation towards managing operational risk on a day-to-day basis. The researcher aims at building a research model that would be of interest and use to policymakers, regulators and those in charge of the banking corporate governance. In particular, this model is expected to contribute to the area of operational risk mitigation in the banking sector.

How do the UAE commercial banks mitigate their operational risk exposures?	
Definition of Operational Risk	
Source of definition	Basel II
Specific risk exclusions	Market, credit, strategic, reputational
Level of understanding	Good
Operational Risk Management in the Organisation	
Corporate OR unit reporting lines	Group Risk
Internal Audit reporting lines	Group Risk
Relationship: OR vs. Internal Audit	Close
Size of Corporate OR Unit	4 persons
Establishment of Corporate OR Unit	2008
Use of Business Unit ORM	Well developed 6 persons
Business Unit ORM reporting lines	Local Management
Relationship: Business Unit ORM vs. Corporate OR unit	Close
OR Committee	Yes, several
Other OR roles	Part time risk officers
Role of Corporate Operational Risk Function	
Policy setting	Yes
Monitoring function	Yes
Scope of role	All operational risks
Custodians of the framework	Yes
Assurance on 'key' risks	Implicit in role

Aggregating OR's	Yes
Mitigating OR's which span the Business Unit	No
Maintenance of loss data base	Yes
Corporate Operational Risk Unit works with Business Unit ORM	Very often
Corporate Operational Risk Unit works with Business Units	Occasionally
ORM Techniques	
Framework in place	Yes
Type of approach	Bottom up
Extent of coverage	One cycle completed
Change management projects	Separate process
Loss database	Yes
Key risk indicators (KRI's)	Yes
Framework – Data Output	
Business Unit	
Objectives	Yes
Materiality threshold	Yes
Identification	
Risk – description	No
Risk – event/cause	Yes
Risk category	Yes
Recording whether the risk has been experienced	Yes
Assessment	
Likelihood	Yes
Financial impact	Yes
Consequential impact	No
Mitigation	
Assessment of controls in place	Yes
Indicators to monitor	Yes
Action plans	Yes
Implementation date	Yes
Operational Risk Identification	
Responsibility	Business Unit
Support	When required
Focus	Management concerns, BU objectives and processes
Instrument	Framework
Process	Workshop Material events Product development. Software IA process Risk indicators
Data source	People Internal loss data Specialised organisations.
Output	List of risks
Operational Risk Appraisal	
Responsibility	Business Unit Corporate Operational Risk Function: (health-check)
Support Instrument	When required Framework

Process	Workshop IA process: challenging Operational risk (health-check)
Likelihood focus Impact focus	Probability: 1 5 scale AED: 1 6 scale Probability.> AED1m: 1 - 4 scale
Data sources	People Current mitigants Loss Database Risk indicators Software Specialised organisations
Output	Risk rating on a scale of 1-8
Operational Risk Mitigation	
Responsibility	Business Unit
Support	When required
Factors influencing support	Control issue Complexity of risk Seeking best practice
Mitigation – Tactics	
Terminate	Yes Leading edge technology Critical supplier
Treat	Yes Process improve Training Procedure guidelines Exception reports
Take	Yes Cost/benefit
Transfer	Yes Insurance Internal transfer Outsourcing
Other	Exploitation
Mitigation: Selection Procedures and follow up	
Decision Maker Escalation Factors	Mainly Business Unit Scale of risk Cost benefit Resources needed
Selection process Factors	Informal Nature of risk Current controls Previous action
Follow-up	Tracking system at Business Unit level with review
Mitigation – Barriers	
Main barriers	Cost and resource

	Ignorance Reputation Change management Timescales Risk appetite
Also noted	-
Related matters	Budget constraints
Quantification	
Methodology	BIA
Time frame for AMA	3 - 5 years
Level of support	Supported
Training	
Approach	Informal
Method	Risk- mapping Framework
Focus	Management
Operational Risk and the Financial Crisis and Dubai Crisis	
The Financial Crises were predictable	Yes
Recurrence Prevention Measures	Robust risk management structures Stress testing OR aware culture Improved corporate governance Effective regulation
Operational Risks that Contributed to the Financial Crises	Large credit growth Reactive ORM strategies Lack of risk appetite framework Weak regulatory framework
The Impact of the Financial Crises on the UAE Commercial Banks	Bad debt accumulation Lack of liquidity for lending Loss in asset value Loss of faith in the banking system Withdrawal of foreign depositors' money
Mitigation of the Operational Risks that Contributed to the Financial Crises	Intervention of the CBUAE by: Supplying liquidity Guaranteeing depositors' money Guaranteeing interbank lending
Stress testing	Not done yet. Planned during the next year.

Case Study Report: Bank Delta

Bank Specific Details	
Name of the bank	Alpha
Number of branches	46 in UAE and 9 international
Established	1967
Net profit for the year 2009	AED (512) million
Net profit for year 2010	AED 390 million
Total Assets for year 209.	AED 86.7billion
Total Assets for year 2010.	AED 81.3billion
Number of employees	1416
OR current approach	BIA

Introduction: Operational risk is an area that is not researched in the UAE, and is of growing importance to financial institutions because of regulatory requirements. The study examines an uncharted area in the UAE with a practical orientation towards managing operational risk on a day-to-day basis. The researcher aims at building a research model that would be of interest and use to policymakers, regulators and those in charge of the banking corporate governance. In particular, this model is expected to contribute to the area of operational risk mitigation in the banking sector.

How do the UAE commercial banks mitigate their operational risk exposures?	
Definition of Operational Risk	
Source of definition	Basel II
Specific risk exclusions	Market, credit, strategic, reputational
Level of understanding	Good
Operational Risk Management in the Organisation	
Corporate OR unit reporting lines	Group Risk
Internal Audit reporting lines	Group Risk
Relationship: OR vs. Internal Audit	Close
Size of Corporate OR Unit	3 persons
Establishment of Corporate OR Unit	2009
Use of Business Unit ORM	Just started 2 Persons
Business Unit ORM reporting lines	Local Management
Relationship: Business Unit ORM vs. Corporate OR unit	Close
OR Committee	Yes, one
Other OR roles	None
Role of Corporate Operational Risk Function	
Policy setting	Yes
Monitoring function	Yes
Scope of role	All operational risks except environmental risk

Custodians of the framework	Yes
Assurance on 'key' risks	Yes
Aggregating OR's	Yes
Mitigating OR's which span the Business Unit	No
Maintenance of loss data base	No
Corporate Operational Risk Unit works with Business Unit ORM	Developing
Corporate Operational Risk Unit works with Business Units	Developing
ORM Techniques	
Framework in place	Pilot stage
Type of approach	Bottom up
Extent of coverage	Pilot stage
Change management projects	Framework
Loss database	No
Key risk indicators (KRI's)	Yes
Framework – Data Output	
Business Unit	
Objectives	Yes
Materiality threshold	Yes
Identification	
Risk – description	No
Risk – event/cause	Yes
Risk category	No
Recording whether the risk has been experienced	No
Assessment	
Likelihood	Yes
Financial impact	Yes
Consequential impact	Yes
Mitigation	
Assessment of controls in place	Yes
Indicators to monitor	Yes
Action plans	No
Implementation date	No
Operational Risk Identification	
Responsibility	Business Unit
Support	When required
Focus	Business Unit objectives
Instrument	Framework
Process	Workshop Material events Product development. Interviews Meetings Risk indicators Questionnaires External monitor Strategic plan Software Internal audit process
Data source	People
Output	List of risks
Operational Risk Appraisal	
Responsibility	Business Unit

Support Instrument Process	When required Framework Workshop
Likelihood focus Impact focus	Probability: 1 - 6 scale AED: No. of ranges Consequential impact
Data sources	People Current mitigants Performance indicators Specialised organisations.
Output	Risk report
Operational Risk Mitigation	
Responsibility	Business Unit
Support	When required
Factors influencing support	Control issue Type of risk Scale of risk Business Unit skills lacking
Mitigation - Tactics	
Terminate	Yes Strategic Temporarily avoid
Treat	Yes Internal control framework
Take	Yes Cost/benefit Potential size
Transfer	Yes Insurance Internal transfer
Other	Sharing Relaxation
Mitigation: Selection Procedures and follow up	
Decision Maker Escalation Factors	Mainly Business Unit Scale of risk Cost benefit
Selection process Factors	Informal Nature of risk Current controls
Follow-up	Informal through Internal Audit reviews KPI's Personal objectives.
Mitigation - Barriers	
Main barriers	Cost Ignorance Reputation Changing business environment Time

Also noted	-
Related matters	-
Quantification	
Methodology	BIA
Time frame for AMA	3 - 5 years
Level of support	Mixed, depends on the risk
Training	
Approach	None
Method	None
Focus	None
Operational Risk and the Financial Crisis and Dubai Crisis	
The Financial Crises were predictable	Yes
Recurrence Prevention Measures	Robust risk management structures Stress testing OR aware culture Improved corporate governance Effective regulation
Operational Risks that Contributed to the Financial Crises	Large credit growth Reactive ORM strategies Lack of risk appetite framework Weak regulatory framework
The Impact of the Financial Crises on the UAE Commercial Banks	Bad debt accumulation Lack of liquidity for lending Loss in asset value Loss of faith in the banking system Withdrawal of foreign depositors' money
Mitigation of the Operational Risks that Contributed to the Financial Crises	Intervention of the CBUAE by: Supplying liquidity Guaranteeing depositors' money Guaranteeing interbank lending
Stress testing	Not done yet. Planned during the next year.

Appendix C: Critical Incidents

This Appendix provides a summarised analysis of the critical incidents discussed during the interviews. A brief description of the columns is given below:

Description of incident – the name of the incident together with a short sentence describing what happened.
Type of operational risk – the category of the operational risks that are involved according to Basel II classification (Basel II, p. 257). The figure indicates the type of risk.
Incident sensitivity – private indicates that the incident has remained within the confines of the bank whereas public indicates that the incident has appeared at some time in the public domain.
Supporting information – supporting information refer either to the incident or subsequent actions. The type of supporting information available is quoted although this has not always been seen (mainly due to the sensitivity of what is involved). The incidents have been analysed using the interview material.
How identified – answers the question how the incident was picked up.
Mitigation tactic – identifies which of the four mitigation tactics, take, terminate, transfer, and treat were used to mitigate the risk.
Notes on mitigation – additional information related to the mitigation action.

No.	Type of Operational risk	Incident sensitivity	Supporting information	How identified	Mitigation Tactic	Notes on mitigation
1	**Credit card fraud** – hackers break into the network and capture customer's account information (see also *Appendix A*)					
	External fraud (2)	In public domain	Press reports, internal reports	Bank monitoring Customers	Treat	Mitigation took place at bank and public levels
2	**Foreign exchange dealer** – trader ran up sizeable book and withheld information					
	Internal fraud (1)	Private to the bank	Not know	Informal Networking	Treat	Steps taken to improve the control system
3	**Telephone banking operation** – identification of lack of contingency planning					
	Business Disruption and Systems Failures (6)	Private to the bank	Location of second operation	Recognised By management	Treat	Service is switched between the two operations on a regular basis
4	GCC – payments were being mis-routed by correspondents.					
	Internal fraud (1)	Private to the bank	Internal documents believed to be available	Internal control procedures	Treat	Mitigation of this risk has provided important lessons for possible UAE entry into GCC single currency
5	**File of transaction transferred** – errors in transactions discovered following transfer of a file					
	Execution, Delivery and Process Management (7)	Private to the bank	Internal documents believed to be available	Internal control procedures	Take or Treat	A cost benefit analysis was being undertaken to decide whether to assume the risk (and do no further work) or correct all the deals

6	**Joint venture finance company** – systems were unable to cope with (underestimated) business size					
	Business Disruption and Systems Failures (6)	In public domain	Press reports	Customer complaint	Treat	Competitors were able to learn from this incident and avoid making the same mistake
7	**Electronic payments system** – clerks/managers were able to input instructions and release funds					
	Internal fraud (1)	Private to the bank	Not know	Risk review	Take or Treat	Whilst segregation of duties was introduced, the risk was accepted as a low probability.
8	**Insurance operation** – a catalogue of 'bad management' practices was found					
	Business Practice (4)	Initially private then in public domain	Press reports	Regulators	Treat	A complete recovery programme was setup as well as regulatory fines being imposed
9	**Uncleared cheques** – cash being drawn on checks which have not been cleared					
	External fraud (2)	Private to the bank	Not know	Management information - losses began to rise	Treat	Mitigation was an iterative process as those involved continued to find more ways to beat the system
10	**Office fire** – fire occurred but the business continuity plan did not work					
	Business Disruption (6)	Private to the bank	Internal documents believed to be available	Member of staff	Treat	Mitigation now involves testing the business continuity arrangements
11	**Incorrect payment remittance** – despite supervisory controls in place to prevent this from happening, poor training and communication caused large payment error					
	Execution, Delivery and Process Management (7)	Private to the bank	Internal documents believed to be available	Customer Contact	Take or Treat	Training risk has been identified and assumed for a short period but manifestation of payment risk brought forward the action plan
12	**Main Server unavailability** – several instances of hardware/software being unavailable					
	Business Disruption and Systems Failures (6)	Private to the bank	Internal documents believed to be available	Main Server malfunction	Treat	Ongoing incidents are investigated and the risk and risk mitigants re-assessed
13	**Money laundering** – breakdown in the control environment enabled money to be laundered					
	Execution, Delivery and Process Management (7)	Private to the bank and the banking industry	Not know	Industry process	Treat	Controls had to be improved to protect the bank against any further incidents
14	**Account limit excess** – series of controls had lapsed enabling member of staff to set a large excess on his account					
	Internal fraud (1)	Private to the bank	Internal documents believed to be available	Not know	Treat	Control framework had to be re-established
15	**Wallet fund administration** – unable to provide adequate service following large increase in volumes resulting from ambitious strategy					
	Execution, Delivery and Process Management (7)	Private to the bank	Not know	Customer complaint	Terminate and treat	Risk initially avoided by stopping new business whilst more robust infrastructure was put in place
16	**PBX voice switch** – phone net was hacked as a result of (international) changes made to voice switch which left the system exposed					

	External fraud (2)	Private to the bank	Internal documents, internal material on switchboard	Management information call charges increased	Treat	Project team was established to resolve this issue as a number of external parties were involved
17	**Call Centre** – identification of lack of contingency planning arrangements					
	Business Disruption (6)	Private to the bank	Internal documents believed to be available	Management concern	Treat (being considered)	Risk still exists and a number of options are being considered
18	**Deed store** – halogen gas fire prevention system found to be inoperative					
	Business Disruption (6)	Private to the bank	Location of problem	Competitor Suffered a Deed fire	Treat	Lack of communication meant that this risk had been unwittingly assumed. Major work now in place to install new system

Appendix D: High Level Review Document for Auditing the Operational Risk Framework and Function.

Audit objectives: to evaluate and assess the effectiveness of the Operational Risk Function (ORF) and framework.

1. **Organisation**
   - Establish the nature of the organisational arrangements (e.g. organisation chart for the ORF.
   - Does the (corporate) ORF have a clear reporting line into the Risk Director?
   - Does the (Business Unit) ORF have a clear reporting line into Senior Management in the Business Unit?
   - Describe the organisational links between the corporate ORF and the Business Unit ORF. How does the relationship guarantee that the corporate ORF is made aware of all the important operational risk matters?
   - Are the ORF's adequately staffed? – review the experience and qualifications of those involved.
   - Are Operational Risk committees used to monitor the operations of the ORFs? Review the processes for completeness and ensure that action points are followed.

2. **Objectives**
   - Are the objectives of the (corporate) ORF clearly defined and documented?
   - Do they cover the main functions of the ORF? – policy making, risk-mapping, reporting arrangement, quantification, training, risk database maintenance and so on.
   - Have the objectives been formally approved by the Risk Committee/ Board?

3. **Planning**
   - How is the work of ORF planned in order to achieve their stated objectives?
   - Are there adequate resources in place to achieve the plan?
   - Is there a process in place to review the achievements of the plan?
   - Describe the actions taken when changes to the plan are required – how are priorities established?
   - How successful has the ORF been in achieving the plan?

4. **processes**
   - Does the ORF use a (documented) risk-mapping approach?

- Describe the risk-mapping approach and, in particular, the methods used to capture data on risks – do they appear sufficient?
- Does the risk-mapping approach cover the main phases of the risk management process – identification, appraisal (probability/impact) and mitigation?
- Does the risk-mapping approach extend to all areas of the bank?
- How is the documentation maintained up-to-date?
- Are there sufficient controls within the framework to ensure the resultant output is robust (particularly management controls – this is a particular important point as the process is subjective)?
- Is a loss/incident database maintained?
- How is the data base collected?
- Has a methodology for quantifying operational risk been adopted? Describe the methodology used and how is it ensured that it is in line with the requirements of the Regulators?
- How robust is the quantification methodology and do the results appear consistent with the views of management?

5. Reporting

- Does the ROF procedure produce reports on a regular basis?
- Do the reports include a summary of key risks and key risk indicators for monitoring the level of operational risk?
- Describe the action managements take on the reports where there is an unsatisfactory situation noted – does it appear sufficient?

Appendix E: Checklist for Mitigating Operational Risk

Proactive ORM (risk has not materialised)

1. Has the risk been adequately diagnosed?
   - Related to the business unit objectives?
   - Adequately described?
     a. Risk category.
     b. Scale of risk.
     c. Cross linkage to other risks.
   - Probability assessed?
   - Impact assessed?
   - Current mitigants noted?

2. Assess whether it is feasible to implement any mitigation actions:
   - Should the risk be accepted? If so, why?
   - Should the risk be accepted in the short term? If so, why?
   - If the risk is to be accepted should the risk be re-reviewed at a later date? If so, when?
   - Should the risk be avoided completely? If so, why?

3. Assess the action that may be taken to reduce the impact and/or probability:
   - Has a draft cost/benefit analysis been completed and checked for accuracy? If not, why? Who needs to authorise the expenditure?
   - For operational risks where the impact is high but the probability is low; establish whether transferring part of the impact via insurance is feasible. If not, why?
   - Establish the desired level of risk that the organisation wishes to accept (risk appetite) and the current level that has been established through the probability/impact appraisal. How much work is likely to be involved in removing the 'gap' between the two? Can the work involved to close the 'gap' be managed within the business unit (see point 4 below)? Is a project team required to complete the work (see point 5 below)?

4. Assess whether the mitigation work can be managed within the Business Unit:
   - Should additional 'expertise' be used to help mitigate the risk? If not, why?
   - Establish the action required to reduce the impact/probability (typically this would involve improving the internal control system)? For example, is more documentation required, are more resources required, is more training required, are more supervisory checks required, is a better segregation of duties required, does management reporting need to be enhanced, can other units be involved to share the risk, and so on?

- Establish and document an action plan to effect the necessary changes. Who will be responsible for ensuring the action is carried out?

5. Assess whether the mitigation work needs to be managed by establishing a project team
   - Establish the project team and appoint the project manager.
   - Agree on the terms of reference and develop the project plan.
   - Establish a reporting mechanism to keep the Business Unit management informed of the progress of the mitigation actions.

6. Monitor the progress of the action plan
   - Ensure regular progress reports vis-à-vis the achievement of the action/project plans are in place, if they are not, what is the justification for this?
   - Ensure follow up procedures are in place to take action when progress is considered to be unsatisfactory. Implement procedures as appropriate.
   - When the work is complete, re-appraise the impact/probability in light of the improvements made and ensure the residual is acceptable.
   - Update the risk map accordingly.

Reactive ORM (risk has materialised)

1. Examine the diagnosis of the risk – had it been identified? If so, review:
   - Relationship to business unit objectives.
   - Adequacy of description.
     a. Risk category.
     b. Scale of risk.
     c. Cross linkage to other risks.
   - Adequacy of probability assessment.
   - Adequacy of impact assessment.
   - Adequacy of current mitigants.

2. Update the database with the details of the incident that took place
   - What events caused the risk to materialise?
   - How much direct and indirect loss is involved?
   - What are the key lessons to be learned?
   - Who needs to know about the incident? Prepare a report as necessary.

3. Assess whether it is feasible to implement any mitigation actions:
   - Should the risk be accepted and no further action taken? If so, why?

- If the risk is to be accepted should the risk be re-reviewed at a later date? If so, when?
- Given the reason why the incident happened, is it feasible to avoid the risk completely in the future? If so, why?

4. Assess the action that may be taken to reduce the impact and/or probability and prevent future occurrences:
   - Has a draft cost/benefit analysis been completed and checked for accuracy? If not, why? Who needs to authorise the expenditure?
   - Is there scope for using insurance to transfer part of the impact? If not, why?
   - Review the causes of the incident and assess the additional work required to mitigate the risk down to an acceptable level. How much work is likely to be involved? Can the work involved be managed within the business unit (see point 5 below)? Is a project team required to complete the work (see point 6 below)?

5. Assess whether the mitigation work can be managed within the Business Unit
   - Should additional 'expertise' be used to help mitigate the risk? If not, why?
   - Establish the action required to reduce the impact/probability (typically this would involve improving the internal control system)? For example, is more documentation required, are more resources required, is more training required, are more supervisory checks required, is a better segregation of duties required, does management reporting need to be enhanced, can other units be involved to share the risk, and so on?
   - Establish and document an action plan to effect the necessary changes. Who will be responsible for ensuring the action is carried out?

6. Assess whether the mitigation work needs to be managed by establishing a project team:
   - Establish the project team and appoint the project manager.
   - Agree the terms of reference and develop the project plan.
   - Establish a reporting mechanism to keep the Business Unit management informed of the progress of the mitigation actions.

7. Monitor the progress of the action plan:
   - Ensure regular progress reports vis-à-vis the achievement of the action/project plans are in place, if they are not, what is the justification for this?
   - Ensure follow up procedures are in place to take action when progress is considered to be unsatisfactory. Implement procedures as appropriate.
   - When the work is complete, re-appraise the impact/probability in light of the improvements made and ensure the residual is acceptable.
   - Update the risk map accordingly.

LIST OF REFERENCES

Aabo, T. and Fraser, J. (2007): "*Bringing Risk Management into Boardroom*" Journal of Risk Management, April 2007. p. 30 – 37.

Abad-Romero (2009): "*Accurate VAR Calculated Using Empirical Models*" September 2009. International Journal of Theoretical and Applied Finance.

Abernethy, Margaret, A., Bouwens, J., Van, L., and Laurence (2004): "*Determinants of Control System Design in Divisionalized Firms*" Accounting Review, Vol. 79, No. 3, July 2004.

Association for Computing Machinery - ACM (2005): "*Computing Curricula 2005: the Overview Report*" October 2005.

Adams, J. (1998): "*Risk Management is a Balancing Act*", Association for Project Management, February, p. 18 – 19.

Agarwal, N. (2008): "*Financial Crisis: Market Evolution and Risk Perception*" Journal of Business Systems, Governance and Ethics, Vol. 3, No. 2, July 2008.

Agence France-Presse (2008): "*Rogue trader blamed for 4.9 billion Euro Fraud at Société Générale*" Available @: afp.google.com/article/ALeqM5i2qEsuPjTXfhGOQfNtqtvzCumH7w, accessed on July 27, 2010.

Al-Suwaidi, (2010): "*U.A.E. Is Committed to Single Currency Idea.*" March 15, 2010.

Alexander, C. (2005): "*The Present and Future of Financial Risk Management*" ISMA Centre Discussion Paper No. DP2003-12.

Alexander, C. and Sheedy, E. (2005): "*The Professional Risk Managers' Handbook: A Comprehensive Guide to Current Theory and Best Practices*" PRMIA Publications.

Allan, G. (2003): "*A critique of using grounded theory as a research method*" Journal of Business Research Methods, p. 1-10.

Altrichter, H., Feldman, A., Posch, P. and Somekh, B. (2008): "*Teachers investigate their work; an introduction to action research across the professions*" Routledge. p. 147. 2nd ed.

Andersen, A. and Torben J. (2005): "*A Strategic Risk Management Framework for Multinational Enterprise.*" Journal of Business Systems, Governance and Ethics, Vol. 2, No. 1, March 2005.

Andreas, A. (2010): "*The Credit Crisis and Operational Risk - Implications for Practitioners and Regulators*" May 24, 2010. Journal of Operational Risk, Vol. 5, No. 2, Summer, 2010, p. 31.

Andreas, A. (2007): "*The Treatment of Operational Risk under the New Basel Framework - Critical Issues*" Journal of Banking Regulation, August 2007.

Andreas, A. (2007): "*Constraints of Consistent Operational Risk Measurement and Regulation: Data Collection and Loss Reporting.*" Journal of Financial Regulation and Compliance, Feb. 2007.

Andreas A. (2007): "*Constraints of Operational Risk Measurement and the Treatment of Operational Risk under the New Basel Framework.*" Journal of Operational Risk, Vol. 3, No.2, June 2007.

Andreas, A. (2007): "*Data Collection and Loss Reporting*", Journal of Financial Regulation and Compliance, p.11.

Angelos, K. (2005): "*Pure Contagion Effects in International Banking: The case of BCCI's Failure.*" Journal of Applied Economics, Sunday, May 1, 2005.

Annamalah, S, (2008): "*Adoption and Usage of Internet Banking: A Technological Perspective*" December 24, 2008, SSRN: http://ssrn.com/abstract=1320216.

Anton, E. (2005): "*Risk Taking in the Financial Services Industry.*" London: Organisation for Economic Co-operation and Development.

Aref, M. (2009): "*Risk Management Software - Essential Guide*" Journal of Operational Risk, Vol. 4, No.2, Sep. 2009.

Arlington (1998): "*History of decision making*" Available @ http://www.benli.bcc.bilkent.edu.tr/~omer/downloads/dec_analy/history.html, accessed on Aug. 15, 2008.

Arnaboldi, F. and Claeys, P. (2008): "*Financial Innovation in Internet Banking: A Comparative Analysis*" February 15, 2008, SSRN: http://ssrn.com/abstract=1094093.

As-Sardi, A. (2009): "*Evolution of United Arab Emirates Financial Industry*"

Asif, A. (2010): "*Five Steps of Entrepreneurial Decision Making*" Management Decision, Vol. 30, No. 3, p. 211 – 219.

Atkinson, A., Donev, A. and Tobias, R. (2007): "*Optimum Experimental Designs*" Oxford University Press.

Avgouleas, E. (2009): "*What Future for Disclosure as a Regulatory Technique? Lessons from the Global Financial Crisis and Beyond*" March 26, 2009, SSRN: http://ssrn.com/abstract=1369004.

Baert and Carreira (2005): "*Social Theory in the Twentieth Century and Beyond.*" Cambridge, UK: Polity Press.

Bailey, A., Preston M. and Whinston, A. (1981): "*An Application of Complexity Theory to the Analysis of Internal Control Systems*" Auditing: A Journal of Practice and Theory, Vol. No. 1, p. 38 – 52.

Bailey, R. (2008): "*Design of Comparative Experiments*" Cambridge University Press.

Bamberger, A. (2010): "*Technologies of Compliance: Risk and Regulation in a Digital Age*" Texas Review, Vol. 88. 669Berkeley Public Research Paper No. 1463727.

Bank of England – BOA. (2008): "*Financial Banking Industry Stability.*" Report, October 2008. p. 23-25.

Baron, R., and Greenberg, J. (2008): "*Behaviour in organisations.*" 9th ed., Pearson Education Inc., New Jersey: 2008, p. 248.

Basel Committee on Banking Supervision - BCBS (2010): "*International Framework for Liquidity Risk Measurement, Standards and Monitoring.*" BCBS 2010.

Basel Committee on Banking Supervision - BCBS (2010): "*Principles for Enhancing Corporate Governance.*" BCBS 2010.

Basel Committee on Banking Supervision - BCBS (2009): "*Revised international capital framework.*" Consultative proposal, BCBS, January 2009.

Basel Committee on Banking Supervision - BCBS (2009): "*Principles for sound stress testing practices and supervision.*" BCBS 2009.

Basel Committee on Banking Supervision - BCBS (2008): "*Steps to Strengthen the Resilience of the Banking System*" Available @ http://www.bis.org/press/p080416.htm, Accessed on Nov. 6, 2008.

Basel Committee on Banking Supervision - BCBS (2006): "*Guidance on Corporate Governance for Banking Organisations.*" BCBS 2006.

Basel Committee on Banking Supervision - BCBS (2006): "*International Convergence of Capital Measurement and Capital Standards: A Revised Framework, Comprehensive Version*" Bank for International Settlements, June, available at: http://www.bis.org/publ/bcbs128.htm, accessed on March 14, 2008.

Basel Committee on Banking Supervision - BCBS (2006): "*Principles for enhancing corporate governance.*" BCBS consultative document, March 2010.

Basel Committee on Banking Supervision - BCBS (2005a): "*Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework.*" BCBS 2005, Publications No. 118

Basel Committee on Banking Supervision - BCBS (2004): "*International Convergence of Capital Measurement and Capital Standards: A Revised Framework*" BCBS 2005Publications No. 107

Basel Committee on Banking Supervision - BCBS (2003): "*Public Disclosures by Banks: Results of the 2001 Disclosure Survey*" Bank for International Settlements, May 2003.

Basel Committee on Banking Supervision - BCBS (2003): "*Sound Practices for the Management and Supervision of Operational Risk*". Feb. 2003, revised document.

Basel Committee on Banking Supervision - BCBS (2001): "*New Basel Capital Accord – Consultative Document*", Basel Committee on Banking Supervision, January 2001.

Basel Committee on Banking Supervision - BCBS (1999): "*Enhancing Corporate Governance for Banking Organisations.*" BCBS 1999.

Basel Committee on Banking Supervision - BCBS (1998b): "*Framework for Internal Control Systems for Banking Organisations.*" BCBS 1998.

Basel Committee on Banking Supervision - BCBS (1996): "*Amendment to the Capital Accord to Incorporate Market Risks.*" BCBS 1996.

Basel Committee on Banking Supervision - BCBS (1988): "*International convergence of capital measurement and capital standards*" Basel Committee on Banking Supervision, Available @ http://www.bis.org/publ/bcbs04a.htm, accessed on April 27, 2008.

Basi, R.S. (1998): "*Administrative Decision Making: a Contextual Analysis*" Management Decision, Vol. 36, No. 4, p. 23 – 24. In McKinnon, A. (2003): "Decision-Making in Organisations" Journal of Financial Economics 22, p. 201–222.

Basu, D. and Hung, C. (2009): "*The Global Price of Market Risk and Country Inflation.*"

Baxter, P and Jack, S. (2008): "*Qualitative Case Study Methodology: Study design and implementation for novice researchers in The Qualitative Report.*"

Bell, D. (2008): "*Constructing Social Theory.*" Lanham, MD: Rowman and Littlefield.

Bena, J. (2006): "*Information Technology Project Management Risk: The Art and Science.*

Berberoglu, B. (2005): "*An Introduction to Classical and Contemporary Social Theory: A Critical Perspective*" 3rd ed., Lanham, MD: Rowman and Littlefield.

Bernstein, P. (1996): "*The New Religion of Risk Management*" Harvard Business Review, March - April, p. 47 – 51.

Biais, B. (2006): "*Risk Perception and Investment Performance.*" Management Science, Vol. 55, No. 6, p. 118-129, June 2006.

Bigoni and Frid (2008): "*Risk Aversion, Prospect Theory, and Strategic Management*" Working Paper Series in Economics and Finance No. 696.

Michael, E. and Ebert (2009): "*Bank Disclosures under Biases in the Risk Perception of Financial Instruments.*" International Journal of Managerial Finance, Vol. 4, No. 1.

Blommestein and Peters, J. (2009): "*Uncertainty and Risk Management: The Role of Risk (Mis)Management by Financial Institutions*" 28th SUERF Colloquium, Sep. 3, 2009.

Blommaert, J. (2005): "*Discourse.*" Cambridge: Cambridge University Press.

Bonson, E. and Flores, F. (2008): "*Operational Risk Measurement in Banking Institutions: Applying an Agency Framework to Operational Risk Management*" Vol. 17, Issue 4, p. 287-307, Nov. 2008.

Branger, N. and Schlag, C. (2004): "*Model Risk: A Conceptual Framework for Risk Measurement and Hedging.*"

Brindle, M. (1999): "*Games Decision Makers Play*" Management Decision, Vol. 37, No. 8, p. 604 - 612.

British Banking Association and Price Waterhouse Coopers – BBA (1999a): "*Operational Risk Management: The New Frontier.*" Oct. 1999.

Brooks, M. (2002): "*Planning Theory for Practitioners.*" American Planning Association, Chicago, May 2002, p. 175.

Bumiller, E. (2002): "*Bush Signs Bill Aimed at Fraud in Corporations*" The New York Times, available @ http://query.nytimes.com/gst/fupage.html? accessed on Sep. 1, 2009.

Burns, T. and Stalker, G. (1961): "*The Management of Innovation.*" Tavistock, London.

Business Review Weekly (2008): "*Challenges Facing UAE Commercial Banking Industry.*" BRW Report. Oct. 13, 2010.

Cade, E. (2002): "*Managing Banking Risks*" Cambridge: Woodhead.

Calvet, C. (2007): "Bias in Data Analysis." Available @ http://www.laconicsecurity.com/bias-in-data-analysis.html, accessed on April 2, 2009.

Caplan, P. (2004): "*Introduction: Risk Revisited*" Pluto Press: London.

Carpenter, T. (2007): "*Audit Team Brainstorming, Fraud Risk Identification, and Fraud Risk Assessment*" Accounting Review, October 2007.

Carter, M. (2004) "*Review of Contemporary Theories in Management.*" Entrepreneurship Theory and Practice, Vol. 29, Issue 5, p. 89 - 101.

Cash and William C. (2002): "*Credibility, Legitimacy and Boundaries: Linking Research, Assessment and Decision Making.*" KSG Working Papers Series.

CBUAE (2010): "*Banks and Other Financial Institutions Licensed by the CBUAE To Conduct Banking Financial, Investment Brokerage and Money-changing Activities as at 31/12/ 2009*" Available @ http://www.centralbank.ae/en/indcx.php, accessed on Jan. 5, 2010.

CBUAE (2009): "*Basel II and Corporate Culture*" ", Notice 4192/20089 issued on Aug. 3, 2009 to all UAE banks.

CBUAE. (2009): "*UAE Currency Peg to the American Dollar.*" Conference in DFC on Jan. 11, 2009.

CBUAE. (2008): "*Basel II Implementation in the UAE: Operational Risk*", Notice 4170/2008 issued on Dec. 2, 2008 to the UAE banks.

CBUAE (2007): "*The Single Market Program and the GCC Financial Institutes.*"

CBUAE (1990): "*UAE Commercial Banks.*"

CBUAE (1980): "*Federal Law No. (10) of 1980 Concerning the Central Bank, the Monetary System and Organisation of Banking*"

Charmaz, K. (2006): "*Constructing Grounded Theory: A Practical Guide through Qualitative Analysis.*" Thousand Oaks, CA: Sage Publications.

Chaudhury, M. (2009): "*Issues in Operational Risk Capital Modeling.*" September 29, 2009.

Chenail, R. (2003): "*Navigating the C's: Curiosity, Confirmation, Comparison, and Critiquing*" The Qualitative Report, March, Vol. 4, No. 3 and 4, p. 14.

Cheney and Julia S. (2008): "*An Examination of Mobile Banking and Mobile Payments*" June 03, 2008. FRB of Philadelphia - Payment Cards Center Discussion Paper No. 08-07.

Chopra, G. (2009): "*Stress Testing Financial Systems: A Macro Perspective.*" December 29, 2009, SSRN: http://ssrn.com/abstract=1529434.

Ciancanelli, P. and Reyes, G. (2001): "*Corporate Governance in Banking: A Conceptual Framework.*"

Ciborra, C. (2009): "*Why a Spreadsheet Approach Can No Longer Meet Today's Growing Risk Management Needs*" Journal of Management Studies, Vol. 43, Issue 6, September 2009.

Clarke, A. (2005): "*Situational Analysis: Grounded Theory after the Postmodern Turn.*" Thousand Oaks, CA: Sage Publications.

Clarke, D. (2009): "*Bankers warn against accelerating Basel timetable.*" Business Review. Oct. 09, 2009.

Clauss, P., Roncalli, T. (2009): "*Risk Management Lessons from Madoff Fraud.*" March 12, 2009, SSRN: http://ssrn.com/abstract=1358086.

Cohen, L. and Maldonado, A. (2007): "*Research Methods in Education.*" British Journal of Educational Studies. Routledge.

Coleman, L. (2007): "*Risk and Decision Making By Finance Executives: A Survey Study.*" International Journal of Managerial Finance, Vol. 3, No. 1.

Collins and Joseph (2004): "*Design Research: Theoretical and Methodological Issues*" The Journal of the Learning Sciences. p. 15-42.

Committee of Sponsoring Organisations - COSO (2004): "*Enterprise risk management integrated framework.*"

Committee of Sponsoring Organisations - COSO (1992): "*Internal Control – Integrated framework*" September 1992.

Computer Crime Research Center-CCRC (2005): "*Fraud in the Internet.*" Date: April 11, 2005, available @ http://www.crime-research.org/articles/Internet_fraud_0405/, accessed on Aug. 20, 2010.

Corti, L. and Bishop, L. (2005): "*Strategies in Teaching Secondary Analysis of Qualitative Data.*"

Creswell, J. (2003): "*Research design: Qualitative, quantitative, and mixed method approaches.*" Thousand Oaks, CA: Sage Publications.

Currie, C. (2004): "*Basel II and operational risk – Review of Key Concepts*" University of Technology, Sydney - School of Finance and Economics, Operational Risk Forum 25th March, 2004.

Currie, C. (2004): "*The Potential Effect of the New Basel Operational Risk Capital Requirements.*" University of Technology, Sydney - School of Finance and Economics Working Paper No. 137.

Dake, K. (1990): "*Theories of Risk Perception: Who fears What and Why?*" American Academy of Arts and Sciences. Daedalus, Vol. 119, No. 4, p. 41 – 60.

Dean, A. and Shanley, M. (2000): "*New venture survival: Ignorance, external shocks, and risk reduction strategies.*" Journal of Business Venturing Volume 15, Issues 5-6, September-November 2000, p. 393-410

Denzin, N. (2006): "*Sociological Methods: A Sourcebook.*" Aldine Transaction. 5th ed.

Denzin, N. and Lincoln, Y. (2005): "*Introduction: The discipline and practice of qualitative research.*" Thousand Oaks, CA: Sage.

Denzin, N. and Lincoln, Y. (2005): "*The Sage Handbook of Qualitative Research.*" 3rd ed., Thousand Oaks, CA: Sage.

Deventer, and Donald, R. (2004): "*Advanced Financial Risk Management: Tools and Techniques for Integrated Risk Management.*" John Wiley.

Dey, A. and Thomas, Z. (2005): "*Trends in Earnings Management and Informativeness of Earnings Announcements in the Pre- and Post-Sarbanes Oxley Periods.*" Kellogg School of Management, Evanston, Illinois, February, 2005, p.5

Dionne, G. (2005): "*Structured Finance, Risk Management, and the Recent Financial Crisis*" Oct. 13, 2009, SSRN: http://ssrn.com/abstract=1488767, accessed on April8.

Dorfman, S. Dionne, G and Grody, G. (2008): "*Operational Risk and Reference Data: Exploring Costs, Capital Requirements and Risk Mitigation*" Journal of Risk Management, Dec., p. 42 – 51.

Dorfman, S. (1997): "*Introduction to Risk Management.*" 6th ed., Prentice Hall.

Dorfman, S. and Mark, S. (2007): "*Introduction to Risk Management and Insurance.*" 9th ed., Englewood Cliffs, N.J: Prentice Hall, p.9.

Douglas (2009): "*The Failure of Risk Management: Why It's Broken and How to Fix It.*" John Wiley & Sons. p. 46.

Drucker, P. (1997): "*Looking Ahead: Implications of the Present*" Harvard Business Review, September – October 1997, p. 18 – 24.

Dul, J. and Hak, T (2008): "*Case Study Methodology in Business Research*" Oxford: Butterworth- Heinemann.

Dutta, K. and David, F. (2010): "*Scenario Analysis in the Measurement of Operational Risk Capital: A Change of Measure Approach.*" March 4, 2010, SSRN: http://ssrn.com/abstract=1565805.

Echtelt, F., Wynstra, J. and Weele, A. (2006): "*Managing Supplier Involvement in New Product Development: A Multiple-Case Study.*" July 09, 2006.

El-Dyasty, M. (2004): "*Toward a Framework of Expertise Factors in Auditing.*" Journal of Commercial Studies, Vol. 5, No. 3, Nov. 2004.

Eldomiaty, I. (2005): "*Can Fundamental Analysis Support Shareholder Value in a Transitional Market?*" International Business & Economics Research Journal, Vol. 5, No. 1.

Elliott, L. (2008): "*The Gods That Failed: How Blind Faith in Markets Has Cost Us Our Future*" The Bodley Head.

Etay, K. (2008): "*The Credit Crunch: The Regulatory Way Forward*", Law and Financial Markets Review, Vol. 2, No. 3.

Fayol, H. (1919): "*Administration industrielle et générale*" London: Pitman.

Fayol, H. (1949): "*General and Industrial Management*" London: Pitman.

Federal Deposit Insurance Corporation-FDIC (2010): "*Failed Bank List.*" available @ http://www.fdic.gov/bank/individual/failed/banklist.html, accessed on Jan. 5, 2011.

Financial Stability Forum - FSF (2008): "*Report of the Financial Stability Forum on Enhancing Market and Institutional Resilience.*"

Finken, and Silke N. (2004): "*Operational Risk and Insurance: Quantitative and Qualitative Aspects.*" EFMA 2004 Basel Meetings Paper.

Fioretti, G. (2008): "*Either. Or: Exploration of an Emerging Decision Theory.*" December 10, 2008, SSRN: http://ssrn.com/abstract=1314352.

Firebaugh, G. (2008): "*Seven Rules for Social Research.*" Princeton University Press.

Fischer, C. (2005): "*Qualitative research methods: Introduction through empirical studies.*" Academic Press.

Flyvbjerg, B. (2006). "*Five Misunderstandings about Case Study Research.*" Qualitative Inquiry, Vol. 12, no. 2, April 2006, p. 219-245.

Flyvbjerg, B. (2001): "*Making Social Science Matter: Why Social Inquiry Fails and How It Can Succeed Again.*" Cambridge: Cambridge University Press, 2001.

Franzoni, A. (2008): "The Changing Nature of Risk." Finance Institute Research Paper No. 08-35.

Freixas, X. and Santomero, A. (2003): "*An Overall Perspective on Banking Regulation.*" March 10, 2003. Economics and Business Working Paper No. 664.

Gee, J. (2005): "*An Introduction to Discourse Analysis: Theory and Method.*" London: Routledge.

George, A. and Bennett, A. (2005). "*Case studies and theory development in the social sciences.*" London, MIT Press 2005.

Gerring, J. (2005): "*Case Study Research.*" New York: Cambridge University Press, p. 37.

Gewei, Y. (2008): "*Transforming Financial Risk Management - Roadmap, Theory, and Computer Applications.*" International Business and Economics Research Journal, Vol. 4, No. 2.

Ghurair, A. (2009): "*Strategic Challenges for the GCC Banking Industry in the New Millennium*" Al-Baian, July 15, 2009 Iss.

Glaser, B. (2005): "*The Grounded Theory Perspective III: Theoretical coding.*" Sociology Press.

Glasser, W. (1990): "*Control Theory.*" The Quality School, Harper and Row.

Gold, G and Feldman, P. (2008) "*A House of Cards - From Fantasy Finance to Global Crash*", London, Lupus Books.

Gomez, M. and Luis R. (2008): "*Management: People, Performance, Change*" 3rd ed., New York USA: McGraw-Hill. p.19.

Gorrod, M. (2004): "*Risk Management Systems: Technology Trends (Finance and Capital Markets).*" Basingstoke: Palgrave Macmillan.

Graham, M. (2008): "*Warped Geographies of Development: The Internet and Theories of Economic Development.*" Journal of Financial Economics 68, p. 112–126.

Green, B. and Reinstein, A. (2004): "*Banking Industry Financial Statement Fraud and the Effects of Regulation Enforcement and Increased Public Scrutiny.*" Research in Accounting Regulation, Vol. 17, 2004.

Gremler, D. (2004): "*The Critical Incident Technique in Service Research.*" Journal of Service Research, 2004.

Grody and Toms (2009): "*Risk Accounting - A Next Generation Risk Management System for Financial Institutions.*" SSRN: http://ssrn.com/abstract=1395912.

Grody, D., Harmantzis, F. and Kaple, G. (2007): "*Operational Risk and Reference Data: Exploring Costs, Capital Requirements and Risk Mitigation*"

Guba, E. and Lincoln, Y. (2005): "*Competing Paradigms in Qualitative Research*". In Denzin, N.K. and Lincoln, Y.S. (Eds), Handbook of Qualitative Research, California: Sage.

Gulfnews (2009): "*Gulf Review: Currency Peg.*" Jan. 12, 2009 Iss.

Gulfnews (2008): "*Banks Ignore Calls to Clean up Their Acts*", March 18, 2008 Iss.

Gulfnews (2008): "*Strategies for Staying Ahead in UAE Banking Industry*", Sep.14, 2008 Iss.

Gulfnews (2008): "*UAE Banks Restrict ATM Usage Abroad.*" Sept. 16, 2008 Iss.

Gulfnews (2007): "*Banks Break Rules to Hang onto Customers*" Jan. 7, 2007 Iss.

Gulfnews, (2006): "*UAE Economy Resists Financial Crisis*", June 2, 2006 Iss.

Gummesson, E. (2000): "*Qualitative Methods in Management Research*," California: Sage.

Gumport, M. (2002): "*Conducting Case Study Research in Operations Management.*" Journal of Operations Management, Vol. 21, p. 239 – 256.

Gustafsson, J. (2007): "*Sound Practices for the Management of Operational Risk.*" Journal of Operational Risk, Summer, p. 82–93.

Hammond, J., Keeney, R. and Raiffa, H. (1998): "*The Hidden Traps in Decision Making.*" Harvard Business Review, September – October 1998, p 47 – 58.

Harris, Z. (1991): "*A Theory of Language and Information: A mathematical approach.*" Oxford & New York: Clarendon Press.

Hatch, M. (2002): "*Organisation Theory: Modern, symbolic, and postmodern perspectives*" 2nd ed., Oxford University Press.

Hazelton, E. (2009): "*Dubai Debt Crisis: Now Banks Investing Billions Face Fresh Crisis.*" Nov. 27, 2009.

Henri, J. and Journeault, M. (2009): "*Revisiting the Link between Management Control Systems and Strategy in Contingency-Based Research.*" January 14, 2009, SSRN: http://ssrn.com/abstract=1327751.

Hentschel, J. (1998): "*Distinguishing between Types of Data and Methods of Collecting Them.*" World Bank Policy Research Working Paper No. 1914.

Hickson, C. and Turner, J. (1996): "*Banking Regulation's Impact on Industry Monopoly and Risk*" Vol. 96, No. 5, p. 34 – 42.

Higgs, D. (2003): "*Review of the role and effectiveness of non-executive directors.*"

Holliday, A. (2007): "*Doing and Writing Qualitative Research.*" 2nd ed., London: Sage Publications.

Holtgrave, D. and Weber, E. (2009): "*Dimensions of Risk Perception for Financial Risks.*" Jan., 05 2009. Risk Analysis, Vol. 13, No. 5, p. 53-58.

Hopkin, P. (2010): "*Fundamentals of Risk Management*" Kogan-Page 2010.

Hubbard, Douglas (2009): "*The Failure of Operational Risk Management: Why It's Broken and How to Fix It.*" John Wiley & Sons.

Huberman, G. (2007): "*Do stock price bubbles influence corporate investment?*" Journal of Financial Economics 66, p. 271–306.

Hughes, H. (2007): "*Critical incident technique: Exploring methods in information literacy research.*" Centre for Information Studies, Charles Sturt University, p. 49-66.

Hull, J. (2006): "*Risk Management and Financial Institutions*" 6th ed., p. 368 – 374.

Hunter, L. and Erin, L. (2008): "*Collaborative Research Trends and Contributing Factors*". American Sociologist.

International Monitory Fund – IMF. (2005): "*Currency Composition of Official Foreign Exchange Reserves.*" The Accumulation of Foreign Reserves.

Institute of Internal Auditors – IIA. (2010): "*Definition of Internal Auditing.*" Available @ http://www.theiia.org/guidance/standards-and-guidance/ippf/definition-of-internal-auditing/?search=definition%20of%20internal%20audit, accessed on Aug. 21, 2010.

Institute of Internal Auditors– IIA. (2009): "*Standards and Guidelines for the Professional Practice or Internal Auditing*" Atlantic Springs, Florida: IIA, p. 29.

Investopedia (2010): "*Tier 3 Capital Definition*" available @ http://www.investopedia.com/terms/t/tier3capital.asp, accessed on Nov. 25, 2009.

Ishmael, Stacy-Marie (2005): "*Investors' risk appetite is roaring - but are they biting off more than they can chew?*" Financial Times 27-02-2007 Iss.

James, E. and Robert, J (2009). "*In the wake of the financial crisis: rebuilding the image of the finance industry through trust*" Journal of Financial Transformation 125, 2010, p. 41.

Janesick, V. (1998): "*Stretching Exercises for Qualitative Researchers*" California: Sage.

Jason, O. (2009): "*Administration and Management: An Analysis of Fayol Works.*" Journal of Social Sciences.

Johnstone, B. (2002): "*Discourse Analysis.*" Oxford: Blackwell.

Jokivuolle, E., Kimmo Virolainen, K. and Vahama, O. (2008): "*Macro-model-based stress testing of BCBS capital requirements.*"

Joubish, F. (2009): "*Educational Research.*" Department of Education, Federal Urdu University, Karachi,Pakistan.

Kahenman, D. and Tversky, D. (1979): "*Timid Choices and Bold Forecasts: A Cognitive Perspective on Risk Taking*", Management Science, Vol. 39, No.1, January, p. 17 – 31.

Kaple and Gregory J. (2006): "*Operational Risk and Reference Data: Exploring Costs. Capital Requirements and Risk Mitigation.*" SSRN: http://ssrn.com/abstract=849224.

Kelly, A. (2003): "*Decision Making Using game Theory.*" Cambridge University Press.

Kenneth, K. (2009): "*Project Risk Mitigation Tactics – Advantages and Pitfalls.*"

Kerry, J. and Brown, H. (1992): "*The Origin and Early Years of BCCI*" The BCCI Affair: A Report to the Committee on Foreign Relations, United States Senate. Congress 2nd Session Senate Print.

Kevin, D. (2005): "*Measuring Market Risk.*" John Wiley and Sons 2005.

Khan, S. (2009): "*The GCC Monetary Union: Choice of Exchange Rate Regime.*" Washington DC, USA: Peterson Institute for International Economics.

Kincheloe, J. (2005): "*Critical Constructivism Primer.*" New York: Peter Lang.

Klaus, K. (2004): "*Content Analysis: An Introduction to Its Methodology.*" 2nd ed., Thousand Oaks, CA: Sage.

Krishnamoorthy, G. (2002): "*Towards a General Theory of Internal Audit*" Internal Auditing, April, p. 17 – 20.

Kvale and Brinkman (2008): "*Interviews*" 2nd Edition. Thousand Oaks: SAGE.

Lam, J. (2006): "*Enterprise Risk Management*" Presentation to the Federal Reserve January, p.12.

Lam, J. (2005): "*Enterprise Risk Management: From Incentives to Controls*" Wiley; 1st ed.,

Lavington, .F. (1925): "*An Approach to the Theory of Business Risks*" Economics Journal, June, p. 186 – 199.

Lawrence, N. (2006): "*Social Research Methods: Qualitative and Quantitative Approaches.*" 6th ed., Allyn and Bacon, p. 28.

Leeson, N. (1996): "*Rouge Trader*" London: Warner.

Lequiller, François; Derek, B. (2006): "*Understanding National Accounts.*"

Lilico, A. (2008): "*The causes of the Credit Crunch*" Available @ http://conservativehome.blogs.com/centreright/2008/09/the-causes-of-t.html, accessed on Sep. 27, 2008.

Lindlof, T. and Taylor, B. (2002): "*Qualitative Communication Research Methods.*" 2nd ed., Sage Publications, Thousand Oaks, CA (2002). Sage Publications, Inc.

Lindlof, T. and Taylor, B. (2002): "*Qualitative Communication Research Methods.*" 2nd ed., Sage Publications, Thousand Oaks, CA (2002). Sage Publications, Inc. In Holliday, A. (2007): "Doing and Writing Qualitative Research." 2nd Edition. London: Sage Publications.

Lovaas, P. (2009): "*A Comprehensive Information Technology Risk Assessment Framework for Financial Institutions.*"

Lurie, N. (2004): "*Decision Making in Information-Rich Environments: The Role of Information Structure.*" Journal of Consumer Research, Vol. 30, p. 473-486, March 2004.

Macionis and Ken (2008): "*Sociology. A Global Introduction.*" 3rd ed., Harlow: Pearson Education. p.12.

Mahoney, J. and Goertz, G. (2006): "*A Tale of Two Cultures: Contrasting Quantitative and Qualitative Research.*" p. 227–249.

Malphrus, S. (2009): "*Perspectives on Retail Payments Fraud.*" February 11, 2009. Economic Perspectives, Vol.III, No. 1, 2009.

Mansur, Y. (2008): "*The Institutional Stature of the GCC commercial Banking*" Journal of Bank Marketing, Vol. 24, No. 4, p. 171 – 181.

Marrison, C. (2002): "*The Fundamentals of Risk Measurement.*" New York: McGraw Hill, p. 340–342.

Marshall, C. and Rossman, G. (1998): "*Designing Qualitative Research.*" Thousand Oaks, CA: Sage.

Martin, M., Gonzalez, C. and Lebiere, C. (2004): "*Learning to make decisions in dynamic environments.*"

Masli, A. and Peters, G. (2009): "*Examining the Potential Benefits of Internal Control Monitoring Technology.*" December 21, 2009. The Accounting Review, Vol. 85, No. 3.

McCallum, S. (2009): "*COSO Supports improved board Risk Oversight*" Sep.1, 2009 Scott.McCallum@IIA.org. , accessed on June 10, 2010.

McConnell, P. (1998): "*Barings: The Development of a Disaster*" International Journal of Project and Business Risk Management, Vol. 2, Issue 1, p. 59 – 74.

McConnell, P. (1996): "*Information Technology for Market Risk Management in International Banks*" DBA Thesis, Brunel University, July 1996.

McDermott, R., James, H. and Smirnov, O. (2008): "*On the Evolutionary Origin of Prospect Theory Preferences*" Journal of Politics, Vol. 70, No. 2, p. 335-350, April 2008.

McKinnon, A. (2003): "*Decision-Making in Organisations*" Journal of Financial Economics 22, p. 201–222.

McNamee, D. (1997): "*Risk-based Auditing*" Internal Auditor, August, p. 23 – 27.

Merchant, K. (2002): "*The Control Function of Management*" Sloan Management Review, Summer.

Mey, G. and Mruck, K. (2007): "*Grounded Theory Reader.*" HSR-Supplement 19. Cologne, p. 337

Mikes, A. (2008): "*Risk Management at Crunch Time: Are Chief Risk Officers Compliance Champions or Business Partners?*" Journal of Business Systems, Vol. 3, No. 2, July 2008. p. 25,

Millo, Y. and MacKenzie, D. (2008): "*The Usefulness of Inaccurate Models: The Emergence of Financial Risk Management*" Centre for Analysis of Risk and Regulation (CARR) Discussion Papers Series. March 1, 2008.

Millo, Y. and MacKenzie, D. (2007): "*Building a Boundary Object: The Evolution of Financial Risk Management.*" Available @ SSRN: http://ssrn.com/abstract=1031745, accessed on Aug. 25, 2008.

Mintzberg, H. (1989): "*Management*" New York: Free press.

Mitchell, M. and Jolley, J. (2001): "*Research Design Explained.*" 4th ed., New York: Harcourt.

Mok, G. and Hagel, E. (2004): "*Risk patterns in managers' activities.*" Journal of Management, May/June 2004, Vol. 9.

Moosa, I. (2007): "*A Critique of the Advanced Measurement Approach to Regulatory Capital Against Operational Risk*" Department of Accounting and Finance, Monash University-Australia.

Moosa, I. (2007): "*Operational Risk: A Survey of Financial Markets, Institutions & Instruments* " V. 16, No. 4, November. Published by Blackwell Publishing, Inc., p. 168 – 200.

Moosa, I. (2007a): "*Misconceptions about Operational Risk.*" Journal of Operational Risk Winter: pp 97–104.

Moosa, I. (2007b): "*Operational Risk Management*" London: Palgrave.

Muhamat, A. (2009): "*The Mechanisms and Operations of Conventional and Islamic Guarantee Schemes: A Case Study of Credit Guarantee Corporation.*" Banking and Regulation, August 2009.

Mukherjee, K, (2008): "*A Context Dependent Model of Decision Making Under Risk.*" May 23, 2008. INSEAD Working Paper No. 2008/25/DS/EPS.

Mulcaster, W. (2009): "*Strategic F*rameworks" Business Strategy Series, Vol. 10, No 1, p. 68 - 75.

Mustapha, M. (2008): "*Banking in GCC Countries: Performance, Policy environment and Reforms Ahead.*" Banking and Regulation, June 2008.

Nelson, W. (2004): "*Accelerated Testing - Statistical Models, Test Plans, and Data Analysis.*" John Wiley and Sons, New York.

Netter, M. and Poulsen, B., (2003): "*Operational Risk in Financial Service Providers and the Proposed Basel Capital Accord: An Overview.*" January 1, 2003, Journal of Risk, Vol. 1 Iss. 1, p. 37 - 63.

Nielson, L., Kleffner, E. and Ryan B. (2005): "*The Evolution of the Role of Risk Communication in Effective Risk Management.*" Risk Management and Insurance Review. Vol. 8, No. 2, p. 279-289.

Nocera, J. (2009): "*Risk Mismanagement: The Next Ten Di*sasters." The New York Times Magazine.

O'Donoghue, T. and Punch, K. (2003): "*Qualitative Educational Research in Action: Doing and Reflecting.*" Routledge.

Office of the Comptroller of the Currency-OCC, Board of Governors of the Federal Reserve System-FRB, Federal Deposit Insurance Corporation-FDIC, and Office of Thrift Supervision-OTC (2005): "*Results of the 2004 Loss Data Collection Exercise for Operational Risk.*" May 2005.

Oldfield, G. and Santamero, A. (1997): "*Risk Management in Financial institutions*" Sloan Management Review, Autumn.

Ong, M. (1998): "*On the Quantification of Operational Risk*" In Arthur Anderson: Operational Risk and Financial Institutions, London: Risk Publications.

Organisation for Economic Co-operation and Development– OECD (2010): "*Seven EU banks fail stress tests*" July 23, 2010.

ORX Report (2010): "*Operational Risk Exchange Association Report.*" June 2010 issue, available @ http://www.orx.org, accessed on Aug. 7, 2010, p. 32.

Otway, H. and Thomas, K. (2006): "*Reflections on Risk Perception: Philosophy, and the Social and Behavioural Science*s" Journal of Risk, Volume 2, Iss. 2, p. 47 – 114.

Pagach, D. and Richard, S. (2010): "*The Effects of Risk Management on Firm Performance.*" April 10, 2010, SSRN: http://ssrn.com/abstract=1155218.

Palfi, C. (2007): "*A Challenge for Internal Control and Audit in Banking System.*" Accounting and Management Information Systems, L.A.

Palocsay, S. (2008): "*An Excel-Based Decision Support System for Scoring and Ranking Proposed R&D Projects.*" International Journal of Information Technology and Decision Making, Vol. 7, No. 3, p. 56-59.

Parker, D. (2005): "*Revisiting Fayol: Anticipating Contemporary Management.*" British Journal of Management.

Patrick, H. (2010): "*Banks and the budget – lessons from Europe.*" Address by Mr. Patrick Honohan, Governor of the Central Bank & Financial Services, Authority of Ireland, to Renmin University, Beijing, 17 August 2010.

Patton, M. (2002): "*Qualitative research & evaluation methods.*" 3rd ed., Thousand Oaks, CA: Sage Publications.

Patton, M. (2002): "*Qualitative research & evaluation methods.*" 3rd ed. Thousand Oaks, CA: Sage Publications. In Flyvbjerg, B. (2006). "Five Misunderstandings about Case Study Research." Qualitative Inquiry, Vol. 12, No. 2, April 2006, p. 219-245.

Pennington, V. (2008): "*Basel II dead, long live Basel III*", OpRisk & Compliance, 1 Nov. 2008 / Vol. 9 No 11, available @ http://wm2.eim.ae/eim/message.php?folder=INBOX&msgno=5546&nm=200812318554883 89998, accessed on Dec. 3, 2008.

Pereira, D. Oliveira, C. and Fernando, M. (2003): "*The Importance of Communication Skills in Negotiation: An Empirical Study.*" 16th Annual Conference Melbourne, Australia.

Petit, T. (1967): "*A Behavioural Theory of Management*" Academy of Management Journal, Vol. 10, No. 4, p. 341 – 350.

Philips, D. and Nicholas, C. (2000): "*Postpositivism and Educational Research.*" Lanham & Boulder: Rowman and Littlefield Publishers."

Porter, M. (1985): "*Competitive Advantage*" New York: Free Press.

Primus, R. (2008): "Limits of Interpretivism." Harvard Journal of Public Policy; U of Michigan Public Working Paper No. 137.

Purda and Lynnette, D. (2007): "*Risk Perception and the Financial System.*" April 1, 2007. Queen's School of Business Research Paper No. 03-08.

Ragnar, E. (2004): "*Risk Communication and Management in the 21st Century.*" AEI-Brookings Joint Center Working Paper No. 04-10.

Rarick, C. (2003): "*Case Study as Interpretative Research: An Example and Commentary.*" June 2, 2003, SSRN: http://ssrn.com/abstract=1117624.

Rayner, G. and Allen, P. (2008): "*Profile: Rogue trader Jerome Kerviel.*" London: The Telegraph, Sep. 25, 2009.

Recchia, V. (1999): "*Risk Communication and Public Perception of Technological Hazards.*" Working Paper No. 81-99.

Reed, N. (1997): "*Variations on a Theme*" In Value at Risk, Risk Publications.

Rivkin, J. and Siggelkow, N. (*2003*): "*Balancing Search and Stability: Interdependencies among Elements of Organisational Design.*" Management Science, 49, p. 290-311

Robbins, S., and Timothy A. (2008): "*Organisation Behaviour*" 12th ed., Upper Saddle River, New Jersey: Pearson Prentice Hall.

Robbins, S. (2004): "*Organisational Behaviour - Concepts, Controversies, Applications.*" 4th ed., Prentice Hall 2004.

Robert, K. (2009): "*Case Study Research: Design and Methods.*" 4th ed., SAGE Publications. California, 2009.

Robert, L. (1999): "*Recent Developments in Risk Management and Insurance.*" Australian Actuarial Journal, Vol. 5, No. 1, p. 173-184.

Robertson, J. and Austin, G. (2008): "*Do you know where your bank is*?" Shreveport Times.

Rodrigues, C. (2001): "*Fayol's principles of management then and now: A framework for managing today's organisations effectively.*"

Roger, D. (2005): "*Mass Media Research: An Introduction*". 8th ed., Belmont, CA: Wadsworth, 2005.

Rutherford (1998): "*Detailed Scholarly Study Know How.*"

Sabato, G. (2009): "*Financial Crisis: Where did Risk Management Fail*?" Journal of Risk Management, May, p. 50 – 55.

Sadgrove, K. (1996): "*The Complete Guide to Business Risk Management*" London: Gower.

Saif, I. and Choucair, F. (2009): "*Arab Countries Stumble in the Face of Growing Economic Crisis.*" International Journal of Theoretical and Applied Finance, June 2009.

Sandra, E. and Strahan, P. (2004): "*Business Formation and the Deregulation of the Banking Industry.*" Public Policy and the Economics of Entrepreneurship, Vol., p. 59-82.

Sanfey, A. (2007): "*Social Decision-Making: Insights from Game Theory.*" Science 26 October 2007: Vol. 318. no. 5850, p. 598 – 602.

Santos, J. (2000): "*Bank Capital Regulation in Temporary Banking Theory: A Review of the Literature*" Accounting, Auditing and Accountability Journal, Vol. 8, No. 3, p. 202, Sep. 2000.

Scandizo, S. (2005): "*Risk Mapping and Key Risk Indicators in Operational Risk Management*" Journal of Risk Management, Vol. 34, No. 2, p. 231-256, July 2005.

Schiffrin, D., Deborah, T. and Hamilton, H. (2001): "*Handbook of Discourse Analysis.*" Oxford: Blackwell.

Scholz, R. and Tietje, O. (2002): "*Embedded Case Study Methods. Integrating Quantitative and Qualitative Knowledge*" Sage Publications. Thousand Oaks 2002, Sage.

Scott, W. (2007): "*Organisations and Organising: Rational, Natural, and Open Systems Perspectives.*" Pearson Prentice Hall 2007, p. 33

Senior, A. (1999): "*A Modern Approach to Operational Risk*" Risk Professional, Issue 3/1, May, p 24.

Serenko, A. (2006): "*The use of interface agents for email notification in critical incidents.*" International Journal of Human-Computer Studies.

Shadish, W. (2002): "*Experimental and Quasi-Experimental Designs for Generalised Causal Inference.*" Boston: Houghton Mifflin.

Shah, S. and Corley, K. (2006): "*Building Better Theory by Bridging the Quantitative-Qualitative Divide.*" Journal of Management Studies, Vol. 43, No. 8, p. 21- 35.

Shailey, D. (2005) "*The Economic Implications of Outsourcing.*" January 31, 2005, SSRN: http://ssrn.com/abstract=779005.

Sheedy, E. (1999): "*Applying an Agency Framework to Operational Risk Management.*" Journal of Business Research Methods, p. 63 - 78.

Shields, P. and Hassan, T. (2006): "*Intermediate Theory: The Missing Link to Successful Research.*" Journal of Public Affairs Education 12 (3): p. 313–334.

Simon, H. (1997): "*Administrative Behaviour: A Study of Decision-Making Processes in Administrative Organisations*" 4th ed. 1997, Free Press.

Simon, H. (1997): "*The New Service of Management Decision*" New Jersey: Prentice Hall.

Simon, H. (1972): "*Theories of Bounded Rationality.*" In Radner, C. and Radner, R. "*Decision and Organisation*" North Holland Amsterdam.

Simon, K. (2009): "*Dubai Financial Crisis.*" Aug. 12, 2009. Journal of Risk, Volume 2, Iss. 2, p. 25 – 29.

Sloan, A. (2008): "*Using Decision Making Theory to Teach Research Process in the Electronic Age.*" South Carolina Review, Vol. 60, p. 123- 138, University of Baltimore Studies Research Paper No. 2009-06.

Smith, E. (2006): "*Complexity, Networking, and Effects Based Approaches to Operations.*" Administrative Science Quarterly, 47, p. 130.

Smith, M. and Kiwan, E. (2009): "*Dubai seeks debt delay, some units cut to junk*". Reuters, available @ http://www.reuters.com/article/businessNews/idUSTRE5AO4Z120091125, accessed on Nov. 11, 2009.

Sneller, L. (2007): "Sarbanes Oxley Section 404 Costs of Compliance: A Case Study. Corporate Governance: An International Review." Vol. 15, No. 2, p. 101-111.

Soy, S. (2006): "*The case study as a research method*" University of Texas at Austin, 1st ed., 1997.

Spira, L. and Page, M. (2003): "*Risk Management: The Reinvention of Internal Control and the Changing Role of Internal Audit*" Accounting, Auditing and Accountability Journal, Vol. 16, No. 4, p. 251.

Stach, A. and Luis, A. (2010): "*The impact of expectation disconfirmation on customer loyalty and recommendation behaviour.*" Journal of Information Technology Management.

Stake, E. (2005): "*Multiple Case Study Analysis.*" Journal of Business Research Methods, p. 83-101.

Stebbins, R. (2001): "*Exploratory Research in the Social Sciences.*" Thousand Oaks, CA: Sage.

Stemler, S. (2001): "*An Overview of Content Analysis.*" Available @ :http://pareonline.net/getvn.asp?v=7&n=17, accessed on Feb. 22. 2009.

Stoneburner, G. and Feringa, A. (2004): "*Risk Management Guide for Information Technology Systems.*" National Institute of Standards and Technology.

Straits, B. and Singleton, R. (2006): "*Approaches to Social Research.*" 4th ed., Oxford University Press.

Straub, D. and Welke, R. (1998): "*Coping with Systems Risk: Security Planning Models for Managing Decision Making*" MIS Quarterly, December, p. 441 – 469.

Taylor. (2008): "*Corporate Communication of Financial Risk.*" Accounting & Finance. Vol. 50, Iss. 2, p. 17.

Taylor, F. (1911): "*The Principles of Scientific Management.*" In Taylor, F. (1947), "Scientific Management" London: Harper and Row.

Taylor, F. (1947), "*Scientific Management*" London: Harper and Row.

Taylor, G. and Derrick, B. (2007): "*Narratives*" New York University Review of Social Change, Vol. 31, p. 225, 2007.

Tedlow, R. and Purrington, C. (2003): "*The American CEO in the Twentieth Century: Demography and Career Path.*" Harvard Business School Working Paper No. 03-097.

The Public Risk Management Association. (2010): "*A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000*"

The Supervisory Capital Assessment Program-SCAP (2009): "*Stress testing: Design and Implementation.*" Board of Governors of the Federal Reserve System. Published April 24, 2009.

Thomas, G. and James, D. (2006): "*Reinventing grounded theory: some questions about theory, ground and discovery*" British Educational Research Journal, 32, 6, p. 767–795.

Thomas, S. (2004): "*The Function of Measurement in Modern Physical Science.*"

Titus, M. and Lewis, D. (1997): "*Understanding and Applying Value at Risk.*" Value at Risk, Risk Publications, p. 9.

Tiwari, R. and Herstatt, C. (2007): "*Mobile Services in Banking Sector: The Role of Innovative Business Solutions in Generating Competitive Advantage.*" In Proceedings of the International Research Conference on Quality, Innovation and Knowledge Management, New Delhi, p. 886–894.

Tompkins, J. (2005): "*Organisation Theory and Public Management*" Thompson Wadsworth.

Treasury Management Association of Canada (1998): "*Glossary of Risk Management Terms.*"

Tsanakas, and Desli, E. (2007): "*Measurement and Pricing of Operational Risk in Insurance Markets,* SSRN: http://ssrn.com/abstract=1006633.

Tschoegl, A. (2005): "*Foreign Banks in the Pacific*" Journal of Pacific History.

United Arab Emirates Federal Law No. (10) of 1980.

Vanita and Aggarwal (2008): "*Estimating the Accuracy of Value-at-Risk (VAR) in Measuring Risk.*" January 2008. Journal of Operational Risk, Vol. 4, No.3, June 2008.

Venkataraman, S. (2006): "*Integrated Risk Management Framework & Basel-II.*" Available @ SSRN: http://ssrn.com/abstract=882401, accessed on Feb 7, 2009.

Vince, K. (2008): "*Mobile Financial Service Software Description.*" Combined EVD and MFS, July 2008, p. 29.

Virine, L. and Trumper M. (2007): "*Choice of Corporate Risk Management Tools under Moral Hazard.*" Working Paper No. 298.

Wahler, B. (2006): "*Process Managing Operational Risk. Developing a Concept for Adapting Process Management to the Needs of Operational Risk in the Basel II-Framework.*" SSRN: http://ssrn.com/abstract=674221.

Wall Street Journal-WSJ (2009): "*Bank Stress Test FAQ.*" Published Feb. 25, 2009.

Weik, K. (1995): "*What Theory is Not, Theorizing is*" Administrative Science Quarterly, Vol. 40, p. 385 – 390.

Weik, K. (1995): "*What Theory is Not, Theorizing is*", Administrative Science Quarterly, Vol. 40, pp 385 – 390. In Baert and Carreira (2005): "Social Theory in the Twentieth Century and Beyond." Cambridge, UK: Polity Press.

White, D. (1995): "*Application of Systems Thinking to Risk Management: A Review of the Literature*" Management Decisions, Vol. 33, No. 10, p. 35 – 45.

Wikimedia Foundation - WFI (2010): "*Bank Fraud.*" Available @ http://en.wikipedia.org/wiki/Bank_fraud#References, accessed on Aug. 25, 2010.

Wilson, J. and Casu, B. (2009): "*Emerging Themes in Banking: Recent Literature and Directions for Future Research.*" November 2, 2009.

William, R. (2001): "*Institutions and Organisations.*" Journal of Operations Management, Vol. 3, p. 132 – 136.

Woods, M. (2009): "*A Contingency Theory Perspective on the Risk Management Control System.*" Management Accounting Research,

World Fact Book (2010): "*United Arab Emirates Banking and Finance.*" The Library of Congress Country Studies; CIA , available @ http://www.photius.com/countries/united_arab_emirates/economy/united_arab_emirates_economy_banking_and_finance.html, accessed on Sep. 20, 2009.

Yin, R. (2002): "*Case Study Research: Design and Methods*" 3rd ed., Applied Social Research Methods Series, Vol. 5, 24 December 2002.

Yin, R. (2002): "*Case Study Research: Design and Methods*" Third Edition, Applied Social Research Methods Series, Vol. 5, 24 December 2002.In Flyvbjerg, B. (2006). "Five Misunderstandings about Case Study Research." Qualitative Inquiry, vol. 12, no. 2, April 2006, p. 219-245.

Zach, L. (2004): "*Modeling the Information.*"

Zahid, M. and Riaz, Z. (2008): "*Using Case Study Research Method to Emergent Relations of Corporate Governance and Social Responsibility.*" Journal of Quality and Technology Management, Vol. IV, No. 1, p. 9-20, Aug. 6, 2008.

Zainal, A. (2005): "*The Role of an Effective Supervisor: Case Studies at the University of Manchester*" United Kingdom. December 2005.

Zammito, J. (2004): "*A Nice Derangement of Epistemes. Post-positivism in the study of Science.*" Chicago & London: The University of Chicago Press.

Zaugg, A. (2006): "*Online Complaint Management at Swisscom: A Case Study.*" SSRN http://ssrn.com/abstract=1123854.